

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-083138

(43)Date of publication of application : 31.03.1998

(51)Int.Cl.

G09C 1/00

G09C 1/00

H04L 9/08

H04L 9/32

(21)Application number : 08-236528

(71)Applicant : MITSUBISHI ELECTRIC CORP

(22)Date of filing : 06.09.1996

(72)Inventor : HARA YOSHIKI

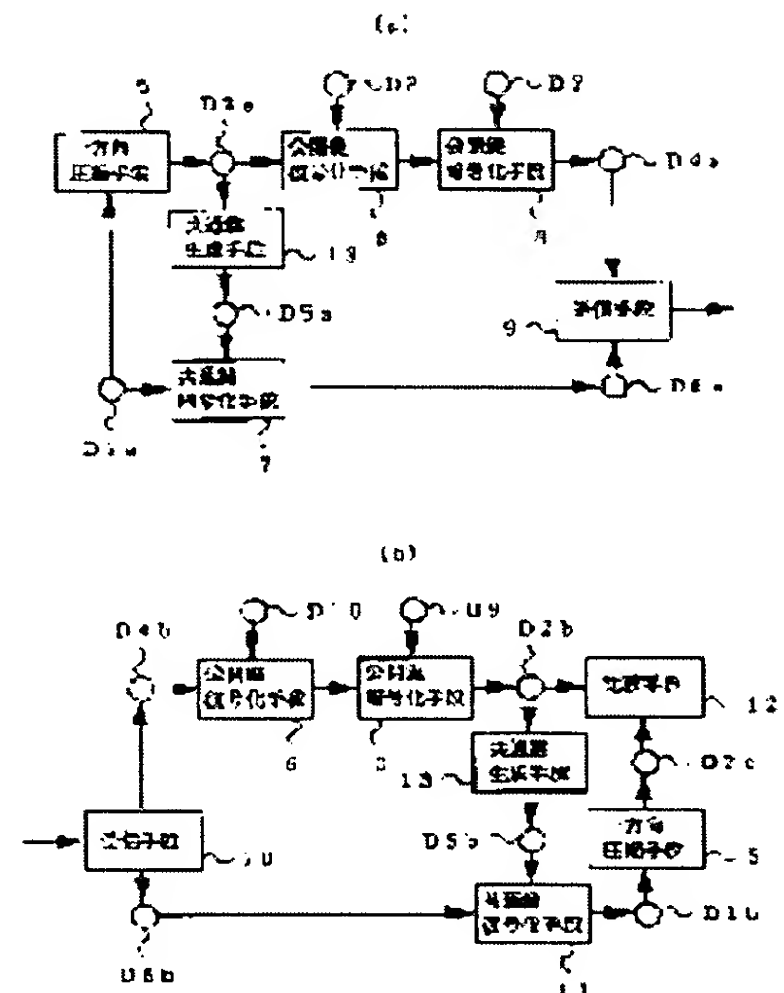
(54) DATA TRANSMISSION METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To eliminate a common key controlling work when a transmitter transmits data to a receiver excepting a transmitter oneself by a common key ciphering transmission data and to automatically generating a common key required for a concealing for a third person from data.

SOLUTION: When the transmitter transmits the data to the receiver excepting the transmitter oneself, that is, when the open key of the receiver is different from the open key of the transmitter, transmitted signature D4a becomes the contents different from a summary D2a becoming the origin generating the open key D5a.

Then, even when the third person having no secret key D10 of the receiver intercepts the signature and the ciphered data while transmitting, the third person can't open key decipher the signature by the secret key D10 of the receiver to can't generate the summary. Thus, since the common key isn't generated from the summary, and the ciphered data aren't common key deciphered, and the data aren't obtained, the contents of the data D1a are concealed for the third person. That is, the attestation of the receiver intended by the transmitter is performed.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

BEST AVAILABLE COPY

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平10-83138

(43)公開日 平成10年(1998) 3月31日

(51)Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G 0 9 C 1/00	6 3 0	7259-5 J	G 0 9 C 1/00	6 3 0 C
		7259-5 J		6 3 0 E
	6 4 0	7259-5 J		6 4 0 B
		7259-5 J		6 4 0 D
		7259-5 J		6 4 0 E
審査請求 未請求 請求項の数 8 O L (全 23 頁) 最終頁に続く				

(21)出願番号 特願平8-236528

(22)出願日 平成8年(1996) 9月6日

(71)出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72)発明者 原 嘉明

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

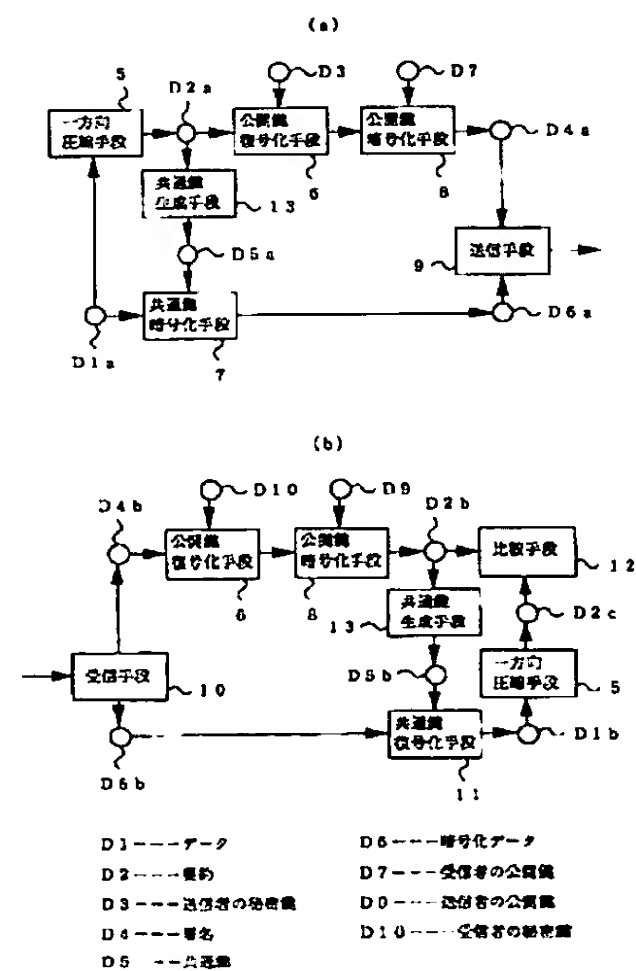
(74)代理人 弁理士 宮田 金雄 (外3名)

(54)【発明の名称】 データ伝送方法

(57)【要約】

【課題】 データの秘匿、送受信者の相互認証、データの一貫性の保証が可能なデータ伝送方法において、共通鍵の管理を不要とする。

【解決手段】 データを一方向圧縮した要約から共通鍵を自動的に生成してデータを共通鍵暗号化し、要約を送信者のみか組み立てられ、かつ受信者のみか翻訳できる署名として送信し、受信した署名から共通鍵を生成してデータを共通鍵復号化し、また署名から生成した要約とデータから生成した要約を比較し、送受信者の相互認証およびデータの一貫性を判定する。



【特許請求の範囲】

【請求項1】 複数のデータ伝送装置が伝送路により接続されて成るネットワーク上で、送信者のデータ伝送装置から受信者のデータ伝送装置にデータを伝送する方法において、所定のデータを一方方向圧縮により生成した要約を送信者の第1の秘密鍵で公開鍵復号化したのち受信者の第1の公開鍵で署名に公開鍵暗号化し、かつ前記要約に基づき第1の共通鍵を生成し、前記所定のデータを前記第1の共通鍵で暗号化データに共通鍵暗号として、前記暗号化データと前記署名とを送信する手順と、上記送信された暗号化データと署名とを受信し、前記署名を受信者の第2の秘密鍵で公開鍵復号化したのち送信者の第2の公開鍵で要約に公開鍵暗号化し、この要約に基づいて第2の共通鍵を生成し、前記受信された暗号化データを前記第2の共通鍵でデータに共通鍵復号化し、このデータを一方方向圧縮により生成した要約と前記署名から生成された要約とを比較して一致した場合に、送受信者の相互認証およびデータの一貫性の保証がされたと判定する手順とを有することを特徴とするデータ伝送方法。

【請求項2】 複数のデータ伝送装置が伝送路により接続されて成るネットワーク上で、送信者のデータ伝送装置から受信者のデータ伝送装置にデータを伝送する方法において、所定のデータを一方方向圧縮により生成した要約を受信者の第1の公開鍵で公開鍵暗号化したのち送信者の第1の秘密鍵で署名に公開鍵復号化し、かつ前記要約に基づき第1の共通鍵を生成し、前記所定のデータを前記第1の共通鍵で暗号化データに共通鍵暗号化して、前記暗号化データと前記署名とを送信する手順と、上記送信された暗号化データと署名とを受信し、この署名を送信者の第2の公開鍵で公開鍵暗号化したのち受信者の第2の秘密鍵で要約に公開鍵復号化し、この要約に基づいて第2の共通鍵を生成し、前記受信された暗号化データを前記第2の共通鍵でデータに共通鍵復号化し、このデータを一方方向圧縮により生成した要約と前記署名から生成された要約とを比較して一致した場合に、送受信者の相互認証およびデータの一貫性の保証がされたと判定する手順とを有することを特徴とするデータ伝送方法。

【請求項3】 複数のデータ伝送装置が伝送路により接続されて成るネットワーク上で、送信者のデータ伝送装置から受信者のデータ伝送装置にデータを伝送する方法において、所定のデータを一方方向圧縮により生成した要約を送信者の第1の秘密鍵で公開鍵復号化したのち受信者の第1の公開鍵で二重に公開鍵暗号化して署名を生成し、前記要約に基づき第1の共通鍵を生成し、前記所定のデータを前記第1の共通鍵で暗号化データに共通鍵暗号化して、前記暗号化データと前記署名とを送信する手順と、上記送信された暗号化データと署名とを受信し、この署名を受信者の第2の秘密鍵で二重に公開鍵復号化したのち送信者の第2の公開鍵で要約に公開鍵暗号化し、この要約に基づいて第2の共通鍵を生成し、前記受

信された暗号化データを前記第2の共通鍵でデータに共通鍵復号化し、このデータを一方方向圧縮により生成した要約と前記署名から生成された要約とを比較して一致した場合に、送受信者の相互認証およびデータの一貫性の保証がされたと判定手順とを有することを特徴とするデータ伝送方法。

【請求項4】 複数のデータ伝送装置が伝送路により接続されて成るネットワーク上で、送信者のデータ伝送装置から受信者のデータ伝送装置にデータを伝送する方法において、所定のデータを一方方向圧縮により生成した要約を受信者の第1の公開鍵で公開鍵暗号化したのち送信者の第1の秘密鍵で公開鍵復号化し、さらに受信者の第1の公開鍵で署名に公開鍵暗号化し、前記要約に基づいて第1の共通鍵を生成し、前記所定のデータを前記第1の共通鍵で暗号化データに共通鍵暗号化して前記暗号化データと前記署名とを送信する手順と、上記送信された暗号化データと署名とを受信し、この署名を受信者の第2の秘密鍵で公開鍵復号化したのち送信者の第2の公開鍵で公開鍵暗号化し、さらに受信者の第2の秘密鍵で要約に公開鍵復号化し、この要約に基づいて第2の共通鍵を生成し、前記受信された暗号化データを前記第2の共通鍵でデータに共通鍵復号化し、このデータを一方方向圧縮により生成された要約と前記署名から生成された要約とを比較して一致した場合に、送受信者の相互認証およびデータの一貫性の保証がされたと判定する手順とを有することを特徴とするデータ伝送方法。

【請求項5】 複数のデータ伝送装置が伝送路により接続されて成るネットワーク上で、送信者のデータ伝送装置から受信者のデータ伝送装置にデータを伝送する方法において、所定のデータを一方方向圧縮により生成した要約を受信者の第1の公開鍵で二重に公開鍵暗号化したのち送信者の第1の秘密鍵で署名に公開鍵復号化し、前記要約に基づいて第1の共通鍵を生成し、前記データを前記第1の共通鍵で暗号化データに共通鍵暗号化して前記暗号化データと前記署名とを送信する手順と、上記送信された暗号化データと署名とを受信し、この署名を送信者の第2の公開鍵で公開鍵暗号化したのち受信者の第2の秘密鍵で二重に公開鍵復号化して要約を生成し、この要約により共通鍵を生成し、前記受信された暗号化データを第2の共通鍵でデータに共通鍵復号化し、このデータを一方方向圧縮により生成した要約と前記署名から生成された要約とを比較して一致した場合に、送受信者の相互認証およびデータの一貫性の保証がされたと判定する手順とを有することを特徴とするデータ伝送方法。

【請求項6】 複数のデータ伝送装置が伝送路により接続されて成るネットワーク上で、送信者のデータ伝送装置から受信者のデータ伝送装置にデータを伝送する方法において、所定のデータを一方方向圧縮により生成した要約を送信者の第1の秘密鍵で中間署名に公開鍵復号化し、この中間署名を受信者の第1の公開鍵で署名に公開

10

20

30

40

50

鍵暗号化し、前記中間署名により第1の共通鍵を生成し、前記データを前記第1の共通鍵で暗号化データに共通鍵暗号化して前記暗号化データと前記署名とを送信する手順と、上記送信された暗号化データと署名とを受信し、この署名を受信者の第2の秘密鍵で中間署名に公開鍵復号化し、この中間署名を送信者の第2の公開鍵で要約に公開鍵暗号化し、前記中間署名により第2の共通鍵に生成し、前記受信された暗号化データを第2の共通鍵でデータに共通鍵復号化し、このデータを一方向圧縮により生成した要約と前記署名から生成された要約とを比較して一致した場合に、送受信者の相互認証およびデータの一貫性の保証がされたと判定する手順とを有することを特徴とするデータ伝送方法。

【請求項7】 複数のデータ伝送装置が伝送路により接続されて成るネットワーク上で、送信者のデータ伝送装置から受信者のデータ伝送装置にデータを伝送する方法において、所定のデータを一方向圧縮により生成した要約を送信者の第1の秘密鍵で公開鍵復号化したのち受信者の第1の公開鍵で中間署名に公開鍵暗号化し、この中間署名を受信者の第1の公開鍵で署名に公開鍵暗号化し、前記中間署名により第1の共通鍵を生成し、前記データを第1の共通鍵で暗号化データに共通鍵暗号化して前記暗号化データと前記署名とを送信する手順と、上記送信された暗号化データと署名とを受信し、この署名を受信者の第2の秘密鍵で中間署名に公開鍵復号化し、この中間署名を受信者の第2の秘密鍵で公開鍵復号化したのち送信者の第2の公開鍵で要約に公開鍵暗号化し、前記中間署名により第2の共通鍵を生成し、前記受信された暗号化データを第2の共通鍵でデータに共通鍵復号化し、このデータを一方向圧縮により生成した要約と前記署名から生成された要約とを比較して一致した場合に、送受信者の相互認証およびデータの一貫性の保証がされたと判定する手順とを有することを特徴とするデータ伝送方法。

【請求項8】 複数のデータ伝送装置が伝送路により接続されて成るネットワーク上で、送信者のデータ伝送装置から受信者のデータ伝送装置にデータを伝送する方法において、所定のデータを一方向圧縮により生成した要約を受信者の第1の公開鍵で公開鍵暗号化したのち送信者の第1の秘密鍵で中間署名に公開鍵復号化し、この中間署名を受信者の第1の公開鍵で署名に公開鍵暗号化し、前記中間署名により第1の共通鍵を生成し、前記データを第1の共通鍵で暗号化データに共通鍵暗号化して、前記暗号化データと前記署名とを送信する手順と、上記送信された暗号化データと署名とを受信し、この署名を受信者の第2の秘密鍵で中間署名に公開鍵復号化し、この中間署名を送信者の第2の公開鍵で公開鍵暗号化したのち受信者の第2の秘密鍵で要約に公開鍵復号化し、前記中間署名により第2の共通鍵を生成し、前記受信された暗号化データを第2の共通鍵でデータに共通鍵

復号化し、このデータを一方向圧縮により生成した要約と前記署名から生成された要約とを比較して一致した場合に、送受信者の相互認証およびデータの一貫性の保証がされたと判定する手順とを有することを特徴とするデータ伝送方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、伝送データの第三者に対する秘匿、送受信者の相互認証、およびデータの一貫性の保証すなわちデータが改ざんされていないことの保証を可能とするデータ伝送方法に関する。

【0002】

【従来の技術】例えば電子メールのようなデータ伝送によって、商取引のデータなどを安全に伝送するためには、伝送データの第三者に対する秘匿、送受信者の相互認証およびデータの一貫性の保証をする必要がある。このため、伝送データの秘匿のために、公開鍵暗号より高速な処理ができる共通鍵暗号を利用し、該共通鍵暗号の共通鍵の秘匿及び送受信者の相互認証のために公開鍵暗号を利用したデータ伝送方法が従来から用いられている。

【0003】図11はこのようなデータ伝送方法が適用されるデータ伝送の説明図であり、1はデータの送信者、2は送信者1の意図するデータの受信者、3は送信者1および受信者2以外の第三者、4はデータの伝送路である。送信者1が受信者2に伝えようとするデータは、送信者1のみが組み立てられ、かつ受信者2のみが翻訳できる形式に変換されて伝送路4を介して伝送される。

【0004】図12は前記従来のデータ伝送方法の説明図、図13は前記従来のデータ伝送方法のフローチャートである。図12および図13において(a)は送信者側、(b)が受信者側の説明図およびフローチャートである。図12(a)において、送信者1が受信者2に伝えようとするデータD1aは例えばハッシュ法による一方向圧縮手段5により要約D2aに一方向圧縮され(処理S1)、該要約D2aは送信者の秘密鍵D3で公開鍵復号化手段6により署名D4aに公開鍵復号化される(処理S2)。

前記データD1aは、送信者により送信者のために「A b c D」や「w X y Z」などのように入力された共通鍵D5aで共通鍵暗号化手段7により暗号化データD6aに共通鍵暗号化される(処理S3)。前記共通鍵D5aは受信者の公開鍵D7で公開鍵暗号化手段8により暗号化共通鍵D8aに公開鍵暗号化される(処理S4)。前記署名D4a、前記暗号化データD6aおよび該暗号化共通鍵D8aは送信手段9により送信される(処理S5)、図12(b)において、受信手段10により署名D4b、暗号化データD6bおよび暗号化共通鍵D8bとして受信される(処理S6)。該署名D4bは送信者の公開鍵D9で公開鍵暗号化手段8により要約

D2 bに公開鍵暗号化される(処理S7)。前記暗号化共通鍵D8 bは受信者の秘密鍵D10で公開鍵復号化手段6により共通鍵D5 bに公開鍵復号化される(処理S8)。前記暗号化データD6 bは該共通鍵D5 bで共通鍵復号化手段11によりデータD1 bに共通鍵復号化され(処理S9)、該データD1 bは一方方向圧縮手段5により要約D2 cに一方方向圧縮される(処理S1)。該要約D2 cと前記要約D2 bは比較手段12により比較され(処理S10)、両者が一致すれば送受信者の相互認証およびデータの一貫性の保証がされたと判定される。

【0005】以上のような従来のデータ伝送方法において、受信者の秘密鍵D10を持たない第三者3が伝送中の署名、暗号化データおよび暗号化共通鍵を傍受しても、暗号化共通鍵を受信者の秘密鍵D10で公開鍵復号化して共通鍵を得ることかできず、暗号化データを共通鍵で共通鍵復号化してデータを得ることかできないため、データD1 aの内容は第三者3に対して秘匿される。すなわち、受信したデータD1 bを翻訳できるのは、送信者1か意図する受信者2のみであり、受信者の認証がなされる。

【0006】また、送信者の秘密鍵D3を持たない第三者3がデータを改ざんしても、改ざんしたデータを一方方向圧縮した要約を送信者の秘密鍵D3で署名に公開鍵復号化することかできない。このため、第三者3が改ざんした署名、暗号化データおよび暗号化共通鍵を受信者2が受信しても、受信された署名D4 bから生成した要約D2 bと受信したデータD1 bから生成した要約D2 cとを比較すると、両者は一致しない。すなわち、署名D4 bから生成した要約D2 bとデータD1 bから生成した要約D2 cが一致すれば、送信者の認証およびデータの一貫性の保証がされたと判定できる。このようにして、伝送データの第三者に対する秘匿、送受信者の相互認証およびデータの一貫性の保証がなされる。

【0007】

【発明が解決しようとする課題】前記従来のデータ伝送方法では、伝送データを第三者に対して秘匿するためには、送信者は少なくとも受信者ごとに異なりかつ第三者には推定しにくい共通鍵を準備し、共通鍵を第三者に対して秘匿し、また第三者による共通鍵推定の試みか成功する危険に備えて、頻繁に共通鍵を変更するなどの管理が必要で、そのため共通鍵の管理のための作業負担が大きいなどの問題点があった。

【0008】この発明の目的は、このような課題を解決するためになされたものであって、共通鍵の管理を不要とすることによって、共通鍵の管理作業の必要をなくしたデータ伝送方法を提供することにある。

【0009】

【課題を解決するための手段】第1の発明に係るデータ伝送方法は、送信者のデータ伝送装置により、データを要約に一方方向圧縮し、該要約を送信者の秘密鍵で公開鍵

復号化したのち受信者の公開鍵で署名に公開鍵暗号化し、前記要約を共通鍵に変換し、前記データを該共通鍵で暗号化データに共通鍵暗号化し、該暗号化データと前記署名とを送信し、受信者のデータ伝送装置により、送信者のデータ伝送装置から送信された暗号化データと署名とを受信し、該署名を受信者の秘密鍵で公開鍵復号化したのち送信者の公開鍵で要約に公開鍵暗号化し、該要約を共通鍵に変換し、前記受信された暗号化データを該共通鍵でデータに共通鍵復号化し、該データを要約に一方方向圧縮し、該要約と前記署名から生成された要約とを比較して一致した場合に、送受信者の相互認証およびデータの一貫性の保証がされたと判定する。

【0010】第2の発明に係るデータ伝送方法は、送信者のデータ伝送装置により、データを要約に一方方向圧縮し、該要約を受信者の公開鍵で公開鍵暗号化したのち送信者の秘密鍵で署名に公開鍵復号化し、前記要約を共通鍵に変換し、前記データを該共通鍵で暗号化データに共通鍵暗号化し、該暗号化データと前記署名とを送信し、受信者のデータ伝送装置により、送信者のデータ伝送装置から送信された暗号化データと署名とを受信し、該署名を送信者の公開鍵で公開鍵暗号化したのち受信者の秘密鍵で要約に公開鍵復号化し、該要約を共通鍵に変換し、前記受信された暗号化データを該共通鍵でデータに共通鍵復号化し、該データを要約に一方方向圧縮し、該要約と前記署名から生成された要約とを比較して一致した場合に、送受信者の相互認証およびデータの一貫性の保証がされたと判定する。

【0011】第3の発明に係るデータ伝送方法は、送信者のデータ伝送装置により、データを要約に一方方向圧縮し、該要約を送信者の秘密鍵で公開鍵復号化したのち受信者の公開鍵で二重に公開鍵暗号化して署名を生成し、前記要約を共通鍵に変換し、前記データを該共通鍵で暗号化データに共通鍵暗号化し、該暗号化データと前記署名とを送信し、受信者のデータ伝送装置により、送信者のデータ伝送装置から送信された暗号化データと署名とを受信し、該署名を受信者の秘密鍵で二重に公開鍵復号化したのち送信者の公開鍵で要約に公開鍵暗号化し、該要約を共通鍵に変換し、前記受信された暗号化データを該共通鍵でデータに共通鍵復号化し、該データを要約に一方方向圧縮し、該要約と前記署名から生成された要約とを比較して一致した場合に、送受信者の相互認証およびデータの一貫性の保証がされたと判定する。

【0012】第4の発明に係るデータ伝送方法は、送信者のデータ伝送装置により、データを要約に一方方向圧縮し、該要約を受信者の公開鍵で公開鍵暗号化したのち送信者の秘密鍵で公開鍵復号化し、さらに受信者の公開鍵で署名に公開鍵暗号化し、前記要約を共通鍵に変換し、前記データを該共通鍵で暗号化データに共通鍵暗号化し、該暗号化データと前記署名とを送信し、受信者のデータ伝送装置により、送信者のデータ伝送装置から送信

された暗号化データと署名とを受信し、該署名を受信者の秘密鍵で公開鍵復号化したのち送信者の公開鍵で公開鍵暗号化し、さらに受信者の秘密鍵で要約に公開鍵復号化し、該要約を共通鍵に変換し、前記受信された暗号化データを該共通鍵でデータに共通鍵復号化し、該データを要約に一方方向圧縮し、該要約と前記署名から生成された要約とを比較して一致した場合に、送受信者の相互認証およびデータの一貫性の保証がされたと判定する。

【0013】第5の発明に係るデータ伝送方法は、送信者のデータ伝送装置により、データを要約に一方方向圧縮し、該要約を受信者の公開鍵で二重に公開鍵暗号化したのち送信者の秘密鍵で署名に公開鍵復号化し、前記要約を共通鍵に変換し、前記データを該共通鍵で暗号化データに共通鍵暗号化し、該暗号化データと前記署名とを送信し、受信者のデータ伝送装置により、送信者のデータ伝送装置から送信された暗号化データと署名とを受信し、該署名を送信者の公開鍵で公開鍵暗号化したのち受信者の秘密鍵で二重に公開鍵暗号化して要約を生成し、該要約を共通鍵に変換し、前記受信された暗号化データを該共通鍵でデータに共通鍵復号化し、該データを要約に一方方向圧縮し、該要約と前記署名から生成された要約とを比較して一致した場合に、送受信者の相互認証およびデータの一貫性の保証がされたと判定することを特徴とするデータ伝送方法。

【0014】第6の発明に係るデータ伝送方法は、送信者のデータ伝送装置により、データを要約に一方方向圧縮し、該要約を送信者の秘密鍵で中間署名に公開鍵復号化し、該中間署名を受信者の公開鍵で署名に公開鍵暗号化し、前記中間署名を共通鍵に変換し、前記データを該共通鍵で暗号化データに共通鍵暗号化し、該暗号化データと前記署名とを送信し、受信者のデータ伝送装置により、送信者のデータ伝送装置から送信された暗号化データと署名とを受信し、該署名を受信者の秘密鍵で中間署名に公開鍵復号化し、該中間署名を送信者の公開鍵で要約に公開鍵暗号化し、前記中間署名を共通鍵に変換し、前記受信された暗号化データを該共通鍵でデータに共通鍵復号化し、該データを要約に一方方向圧縮し、該要約と前記署名から生成された要約とを比較して一致した場合に、送受信者の相互認証およびデータの一貫性の保証がされたと判定することを特徴とするデータ伝送方法。

【0015】第7の発明に係るデータ伝送方法は、送信者のデータ伝送装置により、データを要約に一方方向圧縮し、該要約を送信者の秘密鍵で公開鍵復号化したのち受信者の公開鍵で中間署名に公開鍵暗号化し、該中間署名を受信者の公開鍵で署名に公開鍵暗号化し、前記中間署名を共通鍵に変換し、前記データを該共通鍵で暗号化データに共通鍵暗号化し、該暗号化データと前記署名とを送信し、受信者のデータ伝送装置により、送信者のデータ伝送装置から送信された暗号化データと署名とを受信し、該署名を受信者の秘密鍵で中間署名に公開鍵復号化

し、該中間署名を受信者の秘密鍵で公開鍵復号化したのち送信者の公開鍵で要約に公開鍵暗号化し、前記中間署名を共通鍵に変換し、前記受信された暗号化データを該共通鍵でデータに共通鍵復号化し、該データを要約に一方方向圧縮し、該要約と前記署名から生成された要約とを比較して一致した場合に、送受信者の相互認証およびデータの一貫性の保証がされたと判定することを特徴とするデータ伝送方法。

【0016】第8の発明に係るデータ伝送方法は、送信者のデータ伝送装置により、データを要約に一方方向圧縮し、該要約を受信者の公開鍵で公開鍵暗号化したのち送信者の秘密鍵で中間署名に公開鍵復号化し、該中間署名を受信者の公開鍵で署名に公開鍵暗号化し、前記中間署名を共通鍵に変換し、前記データを該共通鍵で暗号化データに共通鍵暗号化し、該暗号化データと前記署名とを送信し、受信者のデータ伝送装置により、送信者のデータ伝送装置から送信された暗号化データと署名とを受信し、該署名を受信者の秘密鍵で中間署名に公開鍵復号化し、該中間署名を送信者の公開鍵で公開鍵暗号化したのち受信者の秘密鍵で要約に公開鍵復号化し、前記中間署名を共通鍵に変換し、前記受信された暗号化データを該共通鍵でデータに共通鍵復号化し、該データを要約に一方方向圧縮し、該要約と前記署名から生成された要約とを比較して一致した場合に、送受信者の相互認証およびデータの一貫性の保証がされたと判定することを特徴とするデータ伝送方法。

【0017】

【発明の実施の形態】

実施の形態1、図1はこの発明によるデータ伝送方法の実施の形態1の説明図、図2はこの発明によるデータ伝送方法の実施の形態1のフローチャートである。図1および図2において(a)は送信者側、(b)は受信者側の説明図およびフローチャートである。図1(a)において、送信者が受信者に伝えようとするデータD1aは例えばハッシュ法による一方方向圧縮手段5により要約D2aに一方方向圧縮され(処理S1)、該要約D2aは送信者の秘密鍵D3で公開鍵復号化手段6により公開鍵復号化されたのち受信者の公開鍵D7で公開鍵暗号化手段8により署名D4aに公開鍵暗号化される(処理S2)。前記要約D2aは、例えば先頭の2バイト分を16進数表記の4文字に変換するといった共通鍵生成手段13により共通鍵D5aに変換される(処理S11)。前記データD1aは該共通鍵D5aで共通鍵暗号化手段7により暗号化データD6aに共通鍵暗号化される(処理S3)。前記署名D4aおよび該暗号化データD6aは送信手段9により送信され(処理S5)、図1(b)において、受信手段10により署名D4bおよび暗号化データD6bとして受信される(処理S6)。該署名D4bは受信者の秘密鍵D10で公開鍵復号化手段6により公開鍵復号化されたのち送信者の公開鍵D9で公開鍵

暗号化手段8により要約D2bに公開鍵暗号化される(処理S7)。該要約D2bは共通鍵生成手段13により共通鍵D5bに変換される(処理S11)。前記暗号化データD6bは該共通鍵D5bで共通鍵復号化手段11によりデータD1bに共通鍵復号化され(処理S9)、該データD1bは一方方向圧縮手段5により要約D2cに一方方向圧縮される(処理S1)。該要約D2cと前記要約D2bは比較手段12により比較され(処理S10)、両者が一致すれば送受信者の相互認証およびデータの一貫性の保証がされたと判定される。

【0018】以上のような実施の形態1のデータ伝送方法において、送信者が送信者自身以外の受信者に対してデータ伝送を行った場合、すなわち受信者の公開鍵が送信者の公開鍵と異なる場合、送信される署名D4aは共通鍵D5aを生成する元となる要約D2aと異なる内容となるために、受信者の秘密鍵D10を持たない第三者が伝送中の署名および暗号化データを傍受しても、署名を受信者の秘密鍵D10で公開鍵復号化することができず、要約を生成できない。したがって、要約から共通鍵を生成し、暗号化データを共通鍵復号化してデータを得ることかできないため、データD1aの内容は第三者に対して秘匿される。すなわち、受信したデータD1bを翻訳できるのは、送信者が意図する受信者のみであり、受信者の認証がなされる。

【0019】また、送信者の秘密鍵D3を持たない第三者がデータを改ざんしても、改ざんしたデータを一方方向圧縮した要約を送信者の秘密鍵D3で公開鍵復号化することかできず、署名を生成できない。このため、第三者が改ざんした署名および暗号化データを受信者が受信しても、受信された署名D4bから生成した要約D2bと受信したデータD1bから生成した要約D2cとを比較すると、両者は一致しない。すなわち、署名D4bから生成した要約D2bとデータD1bから生成した要約D2cが一致すれば、送信者の認証およびデータの一貫性の保証がされたと判定できる。

【0020】実施の形態2。図3はこの発明によるデータ伝送方法の実施の形態2の説明図、図2はこの発明によるデータ伝送方法の実施の形態2のフローチャートである。図3および図2において(a)は送信者側、

(b)は受信者側の説明図およびフローチャートである。図3(a)において、送信者が受信者に伝えようとするデータD1aは例えばハッシュ法による一方方向圧縮手段5により要約D2aに一方方向圧縮され(処理S1)、該要約D2aは受信者の公開鍵D7で公開鍵暗号化手段8により公開鍵暗号化されたのち送信者の秘密鍵D3で公開鍵復号化手段6により署名D4aに公開鍵復号化される(処理S2)。前記要約D2aは、例えば先頭の2バイト分を16進数表記の4文字に変換するといった共通鍵生成手段13により共通鍵D5aに変換される(処理S11)。前記データD1aは該共通鍵D5a

で共通鍵暗号化手段7により暗号化データD6aに共通鍵暗号化される(処理S3)。前記署名D4aおよび該暗号化データD6aは送信手段9により送信され(処理S5)、図3(b)において、受信手段10により署名D4bおよび暗号化データD6bとして受信される(処理S6)。該署名D4bは送信者の公開鍵D9で公開鍵暗号化手段8により公開鍵暗号化されたのち受信者の秘密鍵D10で公開鍵復号化手段6により要約D2bに公開鍵復号化される(処理S7)。該要約D2bは共通鍵生成手段13により共通鍵D5bに変換される(処理S11)。前記暗号化データD6bは該共通鍵D5bで共通鍵復号化手段11によりデータD1bに共通鍵復号化され(処理S9)、該データD1bは一方方向圧縮手段5により要約D2cに一方方向圧縮される(処理S1)。該要約D2cと前記要約D2bは比較手段12により比較され(処理S10)、両者が一致すれば送受信者の相互認証およびデータの一貫性の保証がされたと判定される。

【0021】以上のような実施の形態2のデータ伝送方法において、送信者が送信者自身以外の受信者に対してデータ伝送を行った場合、すなわち受信者の公開鍵が送信者の公開鍵と異なる場合、送信される署名D4aは共通鍵D5aを生成する元となる要約D2aと異なる内容となるために、受信者の秘密鍵D10を持たない第三者が伝送中の署名および暗号化データを傍受し、署名を送信者の公開鍵D9で公開鍵暗号化しても、受信者の秘密鍵D10で公開鍵復号化することかできず、要約を生成できない。したがって、要約から共通鍵を生成し、暗号化データを共通鍵復号化してデータを得ることができないため、データD1aの内容は第三者に対して秘匿される。すなわち、受信したデータD1bを翻訳できるのは、送信者が意図する受信者のみであり、受信者の認証がなされる。

【0022】また、送信者の秘密鍵D3を持たない第三者がデータを改ざんし、改ざんしたデータを一方方向圧縮した要約を受信者の公開鍵D7で公開鍵暗号化しても、送信者の秘密鍵D3で公開鍵復号化することかできず、署名を生成できない。このため、第三者が改ざんした署名および暗号化データを受信者が受信しても、受信された署名D4bから生成した要約D2bと受信したデータD1bから生成した要約D2cとを比較すると、両者は一致しない。すなわち、署名D4bから生成した要約D2bとデータD1bから生成した要約D2cが一致すれば、送信者の認証およびデータの一貫性の保証がされたと判定できる。

【0023】実施の形態3。図4はこの発明によるデータ伝送方法の実施の形態3の説明図、図2はこの発明によるデータ伝送方法の実施の形態3のフローチャートである。図4および図2において(a)は送信者側、

(b)は受信者側の説明図およびフローチャートであ

る。図4(a)において、送信者が受信者に伝えようとするデータD1aは例えばハッシュ法による一方向圧縮手段5により要約D2aに一方向圧縮され(処理S1)、該要約D2aは送信者の秘密鍵D3で公開鍵復号化手段6により公開鍵復号化されたのち受信者の公開鍵D7で公開鍵暗号化手段8により二重に公開鍵暗号化され、署名D4aが生成される(処理S2)。前記要約D2aは、例えば先頭の2バイト分を16進数表記の4文字に変換するといった共通鍵生成手段13により共通鍵D5aに変換される(処理S11)。前記データD1aは該共通鍵D5aで共通鍵暗号化手段7により暗号化データD6aに共通鍵暗号化される(処理S3)。前記署名D4aおよび該暗号化データD6aは送信手段9により送信され(処理S5)、図4(b)において、受信手段10により署名D4bおよび暗号化データD6bとして受信される(処理S6)。該署名D4bは受信者の秘密鍵D10で公開鍵復号化手段6により二重に公開鍵復号化されたのち送信者の公開鍵D9で公開鍵暗号化手段8により要約D2bに公開鍵暗号化される(処理S7)。該要約D2bは共通鍵生成手段13により共通鍵D5bに変換される(処理S11)。前記暗号化データD6bは該共通鍵D5bで共通鍵復号化手段11によりデータD1bに共通鍵復号化され(処理S9)、該データD1bは一方向圧縮手段5により要約D2cに一方向圧縮される(処理S1)。該要約D2cと前記要約D2bは比較手段12により比較され(処理S10)、両者が一致すれば送受信者の相互認証およびデータの一貫性の保証がされたと判定される。

【0024】以上のような実施の形態3のデータ伝送方法において、送信者が送信者自身に対してデータ伝送を行った場合でも、すなわち受信者の公開鍵が送信者の公開鍵とおなじ場合でも、送信される署名D4aは共通鍵D5aを生成する元となる要約D2aと異なる内容となるために、受信者の秘密鍵D10を持たない第三者が伝送中の署名および暗号化データを傍受しても、署名を受信者の秘密鍵D10で公開鍵復号化することができず、要約を生成できない。したがって、要約から共通鍵を生成し、暗号化データを共通鍵復号化してデータを得ることかできないため、データD1aの内容は第三者に対して秘匿される。すなわち、受信したデータD1bを翻訳できるのは、送信者が意図する受信者のみであり、受信者の認証かなされる。

【0025】また、送信者の秘密鍵D3を持たない第三者がデータを改ざんしても、改ざんしたデータを一方向圧縮した要約を送信者の秘密鍵D3で公開鍵復号化することかできず、署名を生成できない。このため、第三者が改ざんした署名および暗号化データを受信者が受信しても、受信された署名D4bから生成した要約D2bと受信したデータD1bから生成した要約D2cとを比較すると、両者は一致しない。すなわち、署名D4bから

生成した要約D2bとデータD1bから生成した要約D2cが一致すれば、送信者の認証およびデータの一貫性の保証がされたと判定できる。

【0026】実施の形態4、図5はこの発明によるデータ伝送方法の実施の形態4の説明図、図2はこの発明によるデータ伝送方法の実施の形態4のフローチャートである。図5および図2において(a)は送信者側、

(b)は受信者側の説明図およびフローチャートである。図5(a)において、送信者が受信者に伝えようとするデータD1aは例えばハッシュ法による一方向圧縮手段5により要約D2aに一方向圧縮され(処理S1)、該要約D2aは受信者の公開鍵D7で公開鍵暗号化手段8により公開鍵暗号化されたのち送信者の秘密鍵D3で公開鍵復号化手段6により公開鍵復号化され、さらに受信者の公開鍵D7で公開鍵暗号化手段8により署名D4aに公開鍵暗号化される(処理S2)。前記要約D2aは、例えば先頭の2バイト分を16進数表記の4文字に変換するといった共通鍵生成手段13により共通鍵D5aに変換される(処理S11)。前記データD1aは該共通鍵D5aで共通鍵暗号化手段7により暗号化データD6aに共通鍵暗号化される(処理S3)。前記署名D4aおよび該暗号化データD6aは送信手段9により送信され(処理S5)、図5(b)において、受信手段10により署名D4bおよび暗号化データD6bとして受信される(処理S6)。該署名D4bは受信者の秘密鍵D10で公開鍵復号化手段6により公開鍵復号化されたのち送信者の公開鍵D9で公開鍵暗号化手段8により公開鍵暗号化され、さらに受信者の秘密鍵D10で公開鍵復号化手段6により要約D2bに公開鍵復号化される(処理S7)。該要約D2bは共通鍵生成手段13により共通鍵D5bに変換される(処理S11)。前記暗号化データD6bは該共通鍵D5bで共通鍵復号化手段11によりデータD1bに共通鍵復号化され(処理S9)、該データD1bは一方向圧縮手段5により要約D2cに一方向圧縮される(処理S1)。該要約D2cと前記要約D2bは比較手段12により比較され(処理S10)、両者が一致すれば送受信者の相互認証およびデータの一貫性の保証がされたと判定される。

【0027】以上のような実施の形態4のデータ伝送方法において、送信者が送信者自身に対してデータ伝送を行った場合でも、すなわち受信者の公開鍵が送信者の公開鍵とおなじ場合でも、送信される署名D4aは共通鍵D5aを生成する元となる要約D2aと異なる内容となるために、受信者の秘密鍵D10を持たない第三者が伝送中の署名および暗号化データを傍受しても、署名を受信者の秘密鍵D10で公開鍵復号化することができず、要約を生成できない。したがって、要約から共通鍵を生成し、暗号化データを共通鍵復号化してデータを得ることかできないため、データD1aの内容は第三者に対して秘匿される。すなわち、受信したデータD1bを翻訳

できるのは、送信者が意図する受信者のみであり、受信者の認証かなされる。

【0028】また、送信者の秘密鍵D3を持たない第三者がデータを改ざんし、改ざんしたデータを一方向圧縮した要約を受信者の公開鍵D7で公開鍵暗号化しても、送信者の秘密鍵D3で公開鍵復号化することができず、署名を生成できない。このため、第三者が改ざんした署名および暗号化データを受信者が受信しても、受信された署名D4bから生成した要約D2bと受信したデータD1bから生成した要約D2cとを比較すると、両者は一致しない。すなわち、署名D4bから生成した要約D2bとデータD1bから生成した要約D2cが一致すれば、送信者の認証およびデータの一貫性の保証がされたと判定できる。

【0029】実施の形態5、図6はこの発明によるデータ伝送方法の実施の形態5の説明図、図2はこの発明によるデータ伝送方法の実施の形態5のフローチャートである。図6および図2において(a)は送信者側、

(b)は受信者側の説明図およびフローチャートである。図6(a)において、送信者が受信者に伝えようとするデータD1aは例えばハッシュ法による一方向圧縮手段5により要約D2aに一方向圧縮され(処理S1)、該要約D2aは受信者の公開鍵D7で公開鍵暗号化手段8により二重に公開鍵暗号化されたのち送信者の秘密鍵D3で公開鍵復号化手段6により署名D4aに公開鍵復号化される(処理S2)。前記要約D2aは、例えば先頭の2バイト分を16進数表記の4文字に変換するといった共通鍵生成手段13により共通鍵D5aに変換される(処理S11)。前記データD1aは該共通鍵D5aで共通鍵暗号化手段7により暗号化データD6aに共通鍵暗号化される(処理S3)。前記署名D4aおよび該暗号化データD6aは送信手段9により送信され(処理S5)、図6(b)において、受信手段10により署名D4bおよび暗号化データD6bとして受信される(処理S6)。該署名D4bは送信者の公開鍵D9で公開鍵暗号化手段8により公開鍵暗号化されたのち受信者の秘密鍵D10で公開鍵復号化手段6により二重に公開鍵復号化され、要約D2bが生成される(処理S7)。該要約D2bは共通鍵生成手段13により共通鍵D5bに変換される(処理S11)。前記暗号化データD6bは該共通鍵D5bで共通鍵復号化手段11によりデータD1bに共通鍵復号化され(処理S9)、該データD1bは一方向圧縮手段5により要約D2cに一方向圧縮される(処理S1)。該要約D2cと前記要約D2bは比較手段12により比較され(処理S10)、両者が一致すれば送受信者の相互認証およびデータの一貫性の保証がされたと判定される。

【0030】以上のような実施の形態5のデータ伝送方法において、送信者が送信者自身に対してデータ伝送を行った場合でも、すなわち受信者の公開鍵が送信者の公

開鍵とおなじ場合でも、送信される署名D4aは共通鍵D5aを生成する元となる要約D2aと異なる内容となるために、受信者の秘密鍵D10を持たない第三者が伝送中の署名および暗号化データを傍受し、署名を送信者の公開鍵D9で公開鍵暗号化しても、受信者の秘密鍵D10で公開鍵復号化することができず、要約を生成できない。したかつて、要約から共通鍵を生成し、暗号化データを共通鍵復号化してデータを得ることができないため、データD1aの内容は第三者に対して秘匿される。

すなわち、受信したデータD1bを翻訳できるのは、送信者が意図する受信者のみであり、受信者の認証かなされる。また、送信者の秘密鍵D3を持たない第三者がデータを改ざんし、改ざんしたデータを一方向圧縮した要約を受信者の公開鍵D7で公開鍵暗号化しても、送信者の秘密鍵D3で公開鍵復号化することができず、署名を生成できない。このため、第三者が改ざんした署名および暗号化データを受信者が受信しても、受信された署名D4bから生成した要約D2bと受信したデータD1bから生成した要約D2cとを比較すると、両者は一致しない。すなわち、署名D4bから生成した要約D2bとデータD1bから生成した要約D2cが一致すれば、送信者の認証およびデータの一貫性の保証がされたと判定できる。

【0031】実施の形態6、図7はこの発明によるデータ伝送方法の実施の形態6の説明図、図8はこの発明によるデータ伝送方法の実施の形態6のフローチャートである。図7および図8において(a)は送信者側、

(b)は受信者側の説明図およびフローチャートである。図7(a)において、送信者が受信者に伝えようとするデータD1aは例えばハッシュ法による一方向圧縮手段5により要約D2aに一方向圧縮され(処理S1)、該要約D2aは送信者の秘密鍵D3で公開鍵復号化手段6により中間署名D11aに公開鍵復号化され(処理S12)、該中間署名D11aは受信者の公開鍵D7で公開鍵暗号化手段8により署名D4aに公開鍵暗号化される(処理S13)。前記中間署名D11aは、例えば先頭の2バイト分を16進数表記の4文字に変換するといった共通鍵生成手段13により共通鍵D5aに変換される(処理S14)。前記データD1aは該共通鍵D5aで共通鍵暗号化手段7により暗号化データD6aに共通鍵暗号化される(処理S3)。前記署名D4aおよび該暗号化データD6aは送信手段9により送信され(処理S5)、図7(b)において、受信手段10により署名D4bおよび暗号化データD6bとして受信される(処理S6)。該署名D4bは受信者の秘密鍵D10で公開鍵復号化手段6により中間署名D11bに公開鍵復号化され(処理S15)、該中間署名D11bは送信者の公開鍵D9で公開鍵暗号化手段8により要約D2bに公開鍵暗号化される(処理S16)。前記中間署名D11bは共通鍵生成手段13により共通鍵D5bに変

換される(処理S14)。前記暗号化データD6bは該共通鍵D5bで共通鍵復号化手段11によりデータD1bに共通鍵復号化され(処理S9)、該データD1bは一方方向圧縮手段5により要約D2cに一方方向圧縮される(処理S1)。該要約D2cと前記要約D2bは比較手段12により比較され(処理S10)、両者が一致すれば送受信者の相互認証およびデータの一貫性の保証がされたと判定される。

【0032】以上のような実施の形態6のデータ伝送方法において、送信される署名D4aは共通鍵D5aを生成する元となる中間署名D11aと異なる内容となるために、受信者の秘密鍵D10を持たない第三者が伝送中の署名および暗号化データを傍受しても、署名を受信者の秘密鍵D10で中間署名に公開鍵復号化することができず、要約を生成できない。したがって、要約から共通鍵を生成し、暗号化データを共通鍵復号化してデータを得ることができないため、データD1aの内容は第三者に対して秘匿される。すなわち、受信したデータD1bを翻訳できるのは、送信者が意図する受信者のみであり、受信者の認証がなされる。

【0033】また、送信者の秘密鍵D3を持たない第三者がデータを改ざんし、改ざんしたデータを一方方向圧縮した要約を送信者の秘密鍵D3で中間署名に公開鍵復号化することができず、署名を生成できない。このため第三者が改ざんした署名および暗号化データを受信者が受信しても、受信された署名D4bから生成した要約D2bと受信したデータD1bから生成した要約D2cとを比較すると、両者は一致しない。すなわち、署名D4bから生成した要約D2bとデータD1bから生成した要約D2cが一致すれば、送信者の認証およびデータの一貫性の保証がされたと判定できる。

【0034】実施の形態7、図9はこの発明によるデータ伝送方法の実施の形態7の説明図、図8はこの発明によるデータ伝送方法の実施の形態7のフローチャートである。図9および図8において(a)は送信者側、(b)は受信者側の説明図およびフローチャートである。図9(a)において、送信者が受信者に伝えようとするデータD1aは例えばハッシュ法による一方方向圧縮手段5により要約D2aに一方方向圧縮され(処理S1)、該要約D2aは送信者の秘密鍵D3で公開鍵復号化手段6により公開鍵復号化されたのち受信者の公開鍵D7で公開鍵暗号化手段8により中間署名D11aに公開鍵暗号化され(処理S12)、該中間署名D11aは受信者の公開鍵D7で公開鍵暗号化手段8により署名D4aに公開鍵暗号化される(処理S13)。前記中間署名D11aは、例えば先頭の2バイト分を16進数表記の4文字に変換するといった共通鍵生成手段13により共通鍵D5aに変換される(処理S14)。前記データD1aは該共通鍵D5aで共通鍵暗号化手段7により暗号化データD6aに共通鍵暗号化される(処理S3)。

前記署名D4aおよび該暗号化データD6aは送信手段9により送信され(処理S5)、図9(b)において、受信手段10により署名D4bおよび暗号化データD6bとして受信される(処理S6)、該署名D4bは受信者の秘密鍵D10で公開鍵復号化手段6により中間署名D11bに公開鍵復号化され(処理S15)、該中間署名D11bは受信者の秘密鍵D10で公開鍵復号化手段6により公開鍵復号化されたのち送信者の公開鍵D9で公開鍵暗号化手段8により要約D2bに公開鍵暗号化される(処理S16)。前記中間署名D11bは共通鍵生成手段13により共通鍵D5bに変換される(処理S14)。前記暗号化データD6bは該共通鍵D5bで共通鍵復号化手段11によりデータD1bに共通鍵復号化され(処理S9)、該データD1bは一方方向圧縮手段5により要約D2cに一方方向圧縮される(処理S1)。該要約D2cと前記要約D2bは比較手段12により比較され(処理S10)、両者が一致すれば送受信者の相互認証およびデータの一貫性の保証がされたと判定される。

【0035】以上のような実施の形態7のデータ伝送方法において、送信される署名D4aは共通鍵D5aを生成する元となる中間署名D11aと異なる内容となるために、受信者の秘密鍵D10を持たない第三者が伝送中の署名および暗号化データを傍受しても、署名を受信者の秘密鍵D10で中間署名に公開鍵復号化することができず、要約を生成できない。したがって、要約から共通鍵を生成し、暗号化データを共通鍵復号化してデータを得ることができないため、データD1aの内容は第三者に対して秘匿される。すなわち、受信したデータD1bを翻訳できるのは、送信者が意図する受信者のみであり、受信者の認証がなされる。さらに、同一内容のデータを複数の受信者に対して伝送する場合、すなわち複数の受信者の公開鍵が互いに異なる場合は、中間署名D11aは受信者ごとに異なる内容で生成されるため、中間署名D11aから生成される共通鍵D5aも受信者ごとに異なり、したがって、共通鍵D5aで共通鍵暗号化手段7により生成される暗号化データD6aも受信者ごとに異なる。

【0036】また、送信者の秘密鍵D3を持たない第三者がデータを改ざんしても、改ざんしたデータを一方方向圧縮した要約を送信者の秘密鍵D3で公開鍵復号化することができず、中間署名を生成できないため、署名を生成できない。このため、第三者が改ざんした署名および暗号化データを受信者が受信しても、受信された署名D4bから生成した要約D2bと受信したデータD1bから生成した要約D2cとを比較すると、両者は一致しない。すなわち、署名D4bから生成した要約D2bとデータD1bから生成した要約D2cが一致すれば、送信者の認証およびデータの一貫性の保証がされたと判定できる。

【0037】実施の形態8、図10はこの発明によるデ

ータ伝送方法の実施の形態8の説明図、図8はこの発明によるデータ伝送方法の実施の形態8のフローチャートである。図10および図8において(a)は送信者側、(b)は受信者側の説明図およびフローチャートである。図10(a)において、送信者が受信者に伝えようとするデータD1aは例えばハッシュ法による一方向圧縮手段5により要約D2aに一方向圧縮され(処理S1)、該要約D2aは受信者の公開鍵D7で公開鍵暗号化手段8により公開鍵暗号化されたのち送信者の秘密鍵D3で公開鍵復号化手段6により中間署名D11aに公開鍵復号化され(処理S12)、該中間署名D11aは受信者の公開鍵D7で公開鍵暗号化手段8により署名D4aに公開鍵暗号化される(処理S13)。前記中間署名D11aは、例えば先頭の2バイト分を16進数表記の4文字に変換するといった共通鍵生成手段13により共通鍵D5aに変換される(処理S14)。前記データD1aは該共通鍵D5aで共通鍵暗号化手段7により暗号化データD6aに共通鍵暗号化される(処理S3)。前記署名D4aおよび該暗号化データD6aは送信手段9により送信され(処理S5)、図10(b)において、受信手段10により署名D4bおよび暗号化データD6bとして受信される(処理S6)。該署名D4bは受信者の秘密鍵D10で公開鍵復号化手段6により中間署名D11bに公開鍵復号化され(処理S15)、該中間署名D11bは送信者の公開鍵D9で公開鍵暗号化手段8により公開鍵暗号化されたのち受信者の秘密鍵D10で公開鍵復号化手段6により要約D2bに公開鍵暗号化される(処理S16)。前記中間署名D11bは共通鍵生成手段13により共通鍵D5bに変換される(処理S14)。前記暗号化データD6bは該共通鍵D5bで共通鍵復号化手段11によりデータD1bに共通鍵復号化され(処理S9)、該データD1bは一方向圧縮手段5により要約D2cに一方向圧縮される(処理S1)。該要約D2cと前記要約D2bは比較手段12により比較され(処理S10)、両者が一致すれば送受信者の相互認証およびデータの一貫性の保証がされたと判定される。

【0038】以上のような実施の形態8のデータ伝送方法において、送信される署名D4aは共通鍵D5aを生成する元となる中間署名D11aと異なる内容となるために、受信者の秘密鍵D10を持たない第三者が伝送中の署名および暗号化データを傍受しても、署名を受信者の秘密鍵D10で中間署名に公開鍵復号化することかできず、要約を生成できない。したがって、要約から共通鍵を生成し、暗号化データを共通鍵復号化してデータを得ることかできないため、データD1aの内容は第三者に対して秘匿される。すなわち、受信したデータD1bを翻訳できるのは、送信者か意図する受信者のみであり、受信者の認証かなされる。さらに、同一内容のデータを複数の受信者に対して伝送する場合、すなわち複数

の受信者の公開鍵が互いに異なる場合は、中間署名D11aは受信者ごとに異なる内容で生成されるため、中間署名D11aから生成される共通鍵D5aも受信者ごとに異なり、したがって、共通鍵D5aで共通鍵暗号化手段7により生成される暗号化データD6aも受信者ごとに異なる。また、送信者の秘密鍵D3を持たない第三者がデータを改ざんし、改ざんしたデータを一方向圧縮した要約を受信者の公開鍵D7で公開鍵暗号化しても、送信者の秘密鍵D3で公開鍵復号化することかできず、中間署名を生成できないため、署名を生成できない。このため、第三者が改ざんした署名および暗号化データを受信者か受信しても、受信された署名D4bから生成した要約D2bと受信したデータD1bから生成した要約D2cとを比較すると、両者は一致しない。すなわち、署名D4bから生成した要約D2bとデータD1bから生成した要約D2cが一致すれば、送信者の認証およびデータの一貫性の保証がされたと判定できる。

【0039】

【発明の効果】第1の発明および第2の発明によれば、送信者が送信者自身以外の受信者に対してデータを伝送する場合に、伝送データを共通鍵暗号化して第三者に対して秘匿するために必要な共通鍵は、データから自動的に生成されるため、共通鍵を準備したり、共通鍵を第三者に対して秘匿したり、共通鍵を頻繁に変更するなどの管理が不要となり、共通鍵管理のための作業の必要をなくすることができる。

【0040】第3の発明、第4の発明、第5の発明および第6の発明によれば、送信者が送信者自身に対してデータを伝送する場合にも、伝送データを共通鍵暗号化して第三者に対して秘匿するために必要な共通鍵は、データから自動的に生成されるため、共通鍵を準備したり、共通鍵を第三者に対して秘匿したり、共通鍵を頻繁に変更するなどの管理が不要となり、共通鍵管理のための作業の必要をなくすることができる。

【0041】第7の発明および第8の発明によれば、送信者が送信者自身に対してデータを伝送する場合にも、伝送データを共通鍵暗号化して第三者に対して秘匿するために必要な共通鍵は、データから自動的に生成されるため、共通鍵を準備したり、共通鍵を第三者に対して秘匿したり、共通鍵を頻繁に変更するなどの管理が不要となり、共通鍵管理のための作業の必要をなくすることができる、と同時に、複数の相異なる受信者に同一データを伝送する場合も、受信者ごとに相異なる暗号化データを伝送するため、同一内容が伝送されたことを受信者に対して隠すことができる。

【図面の簡単な説明】

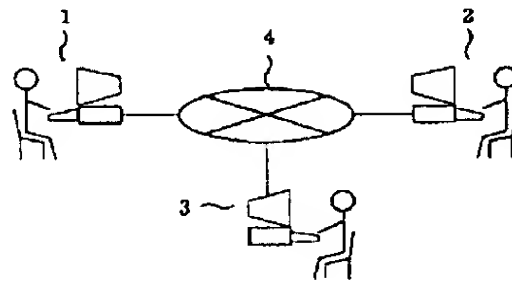
【図1】 この発明の実施の形態1の説明図である。

【図2】 この発明の実施の形態1、実施の形態2、実施の形態3、実施の形態4および実施の形態5のフローチャートである。

【図3】 この発明の実施の形態2の説明図である。
 【図4】 この発明の実施の形態3の説明図である。
 【図5】 この発明の実施の形態4の説明図である。
 【図6】 この発明の実施の形態5の説明図である。
 【図7】 この発明の実施の形態6の説明図である。
 【図8】 この発明の実施の形態6、実施の形態7および実施の形態8のフローチャートである。
 【図9】 この発明の実施の形態7の説明図である。
 【図10】 この発明の実施の形態8の説明図である。
 【図11】 データ伝送の説明図である。
 【図12】 従来のデータ伝送方法の説明図である。
 【図13】 従来のデータ伝送方法のフローチャートである。
 【符号の説明】
 1 送信者、2 受信者、3 第三者、4 伝送路、5 一方向圧縮手段、6 公開鍵復号化手段、7 共通鍵暗号化手段、8 公開鍵暗号化手段、9 送信手段、10 *

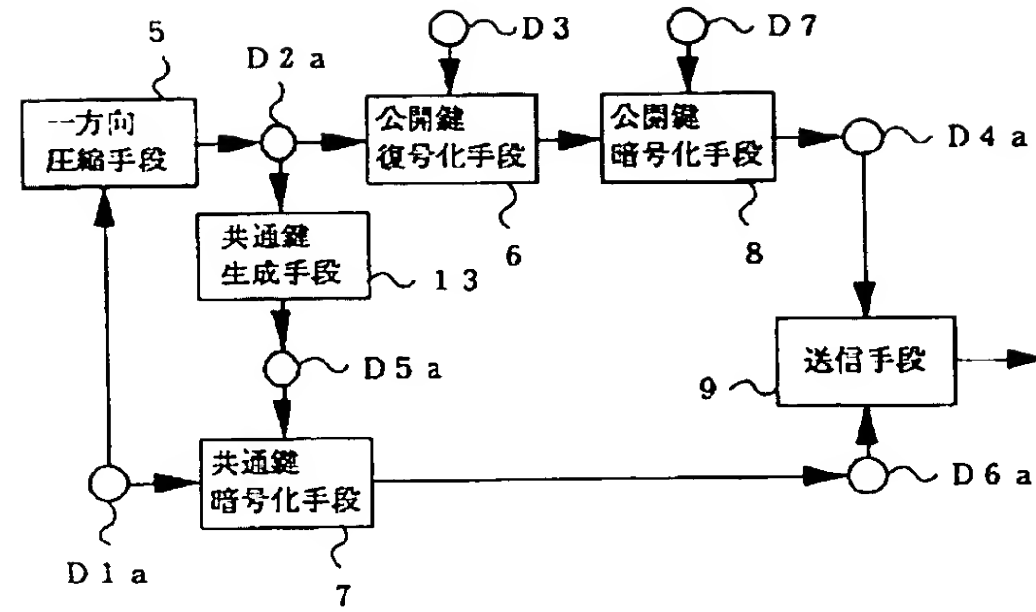
* 送信手段、11 共通鍵復号化手段、12 比較手段、13 共通鍵生成手段、D1 テータ、D2 要約、D3 送信者の秘密鍵、D4 署名、D5 共通鍵、D6 暗号化テータ、D7 受信者の公開鍵、D8 暗号化共通鍵、D9 送信者の公開鍵、D10 受信者の秘密鍵、D11 中間署名、S1 テータから要約を生成する処理、S2 要約から署名を生成する処理、S3 データを暗号化する処理、S4 共通鍵を暗号化する処理、S5 送信処理、S6 受信処理、S7 署名から要約を生成する処理、S8 暗号化共通鍵を復号化する処理、S9 暗号化テータを復号化する処理、S10 比較処理、S11 要約から共通鍵を生成する処理、S12 要約から中間署名を生成する処理、S13 中間署名から署名を生成する処理、S14 中間署名から共通鍵を生成する処理、S15 署名から中間署名を生成する処理、S16 中間署名から要約を生成する処理。

【図11】

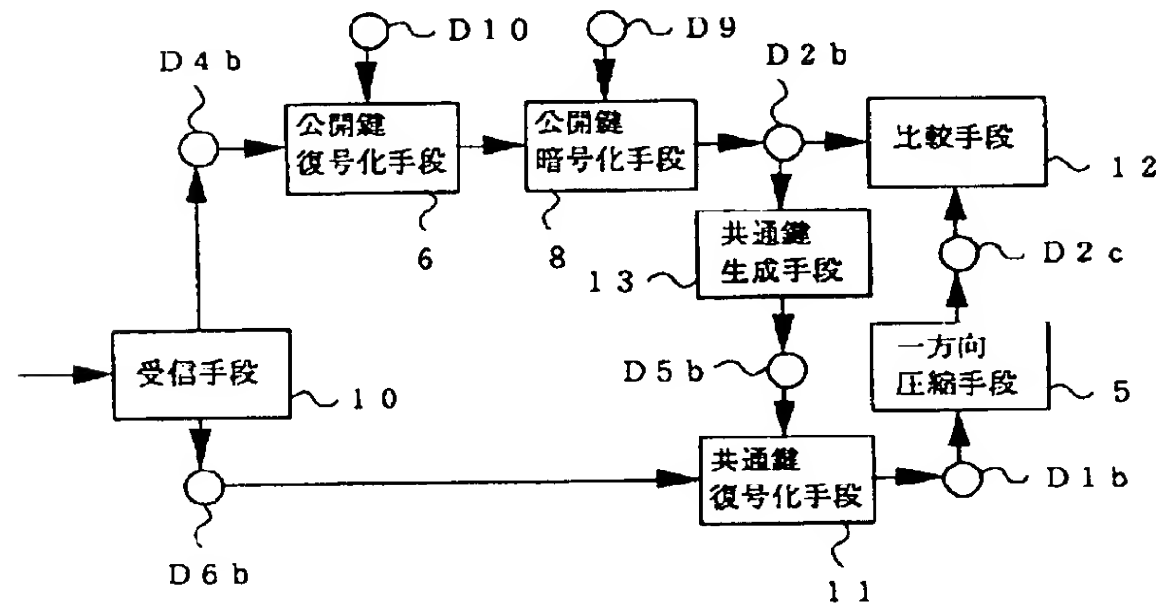


【図1】

(a)



(b)



D1 --- データ

D2 --- 要約

D3 --- 送信者の秘密鍵

D4 --- 署名

D5 --- 共通鍵

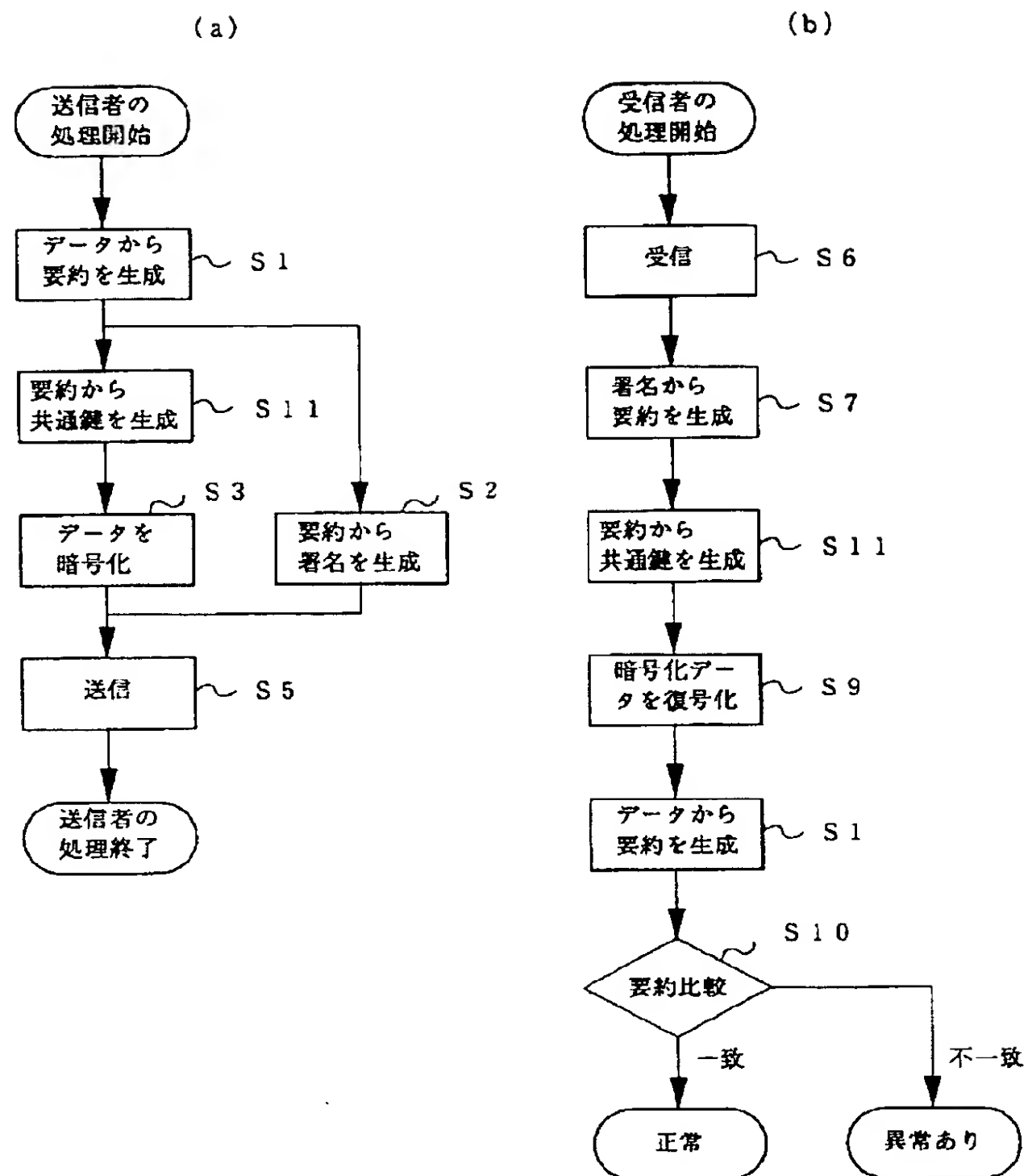
D6 --- 暗号化データ

D7 --- 受信者の公開鍵

D9 --- 送信者の公開鍵

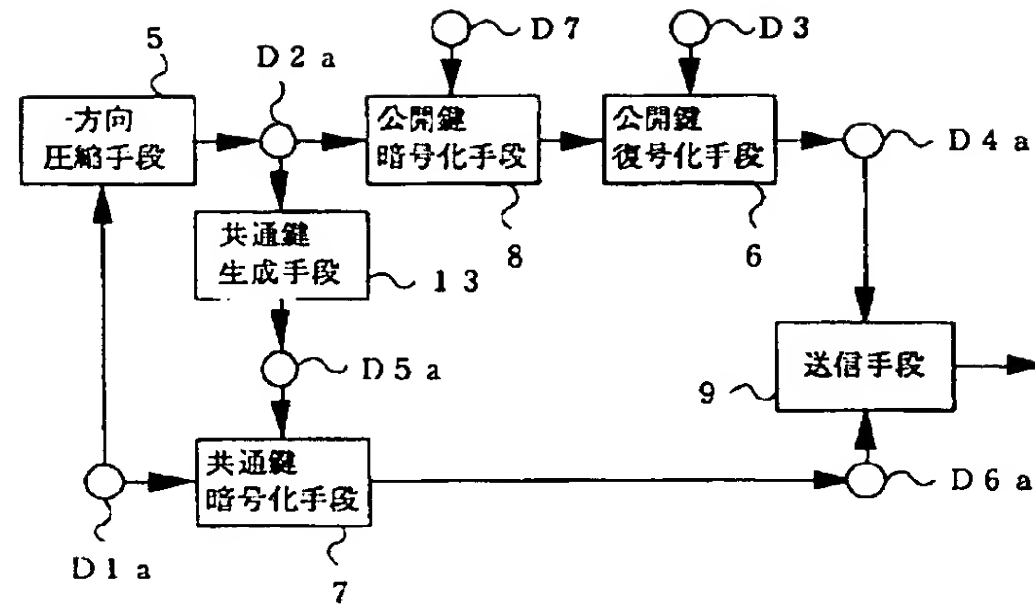
D10 --- 受信者の秘密鍵

【図2】

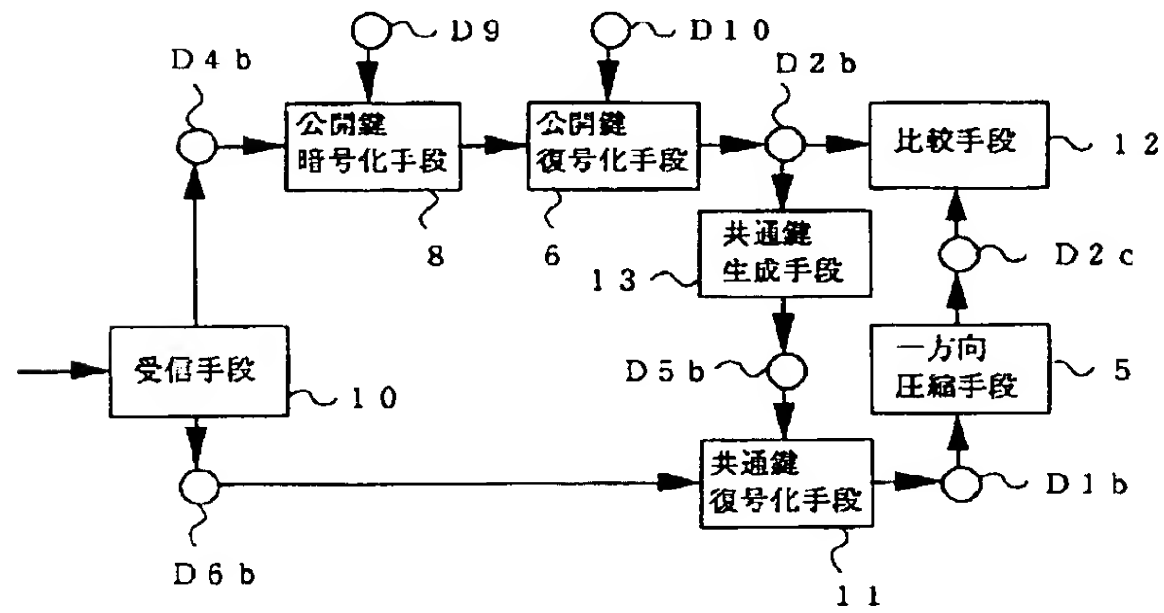


【図3】

(a)



(b)



D1 --- データ

D2 --- 要約

D3 --- 送信者の秘密鍵

D4 --- 署名

D5 --- 共通鍵

D6 --- 暗号化データ

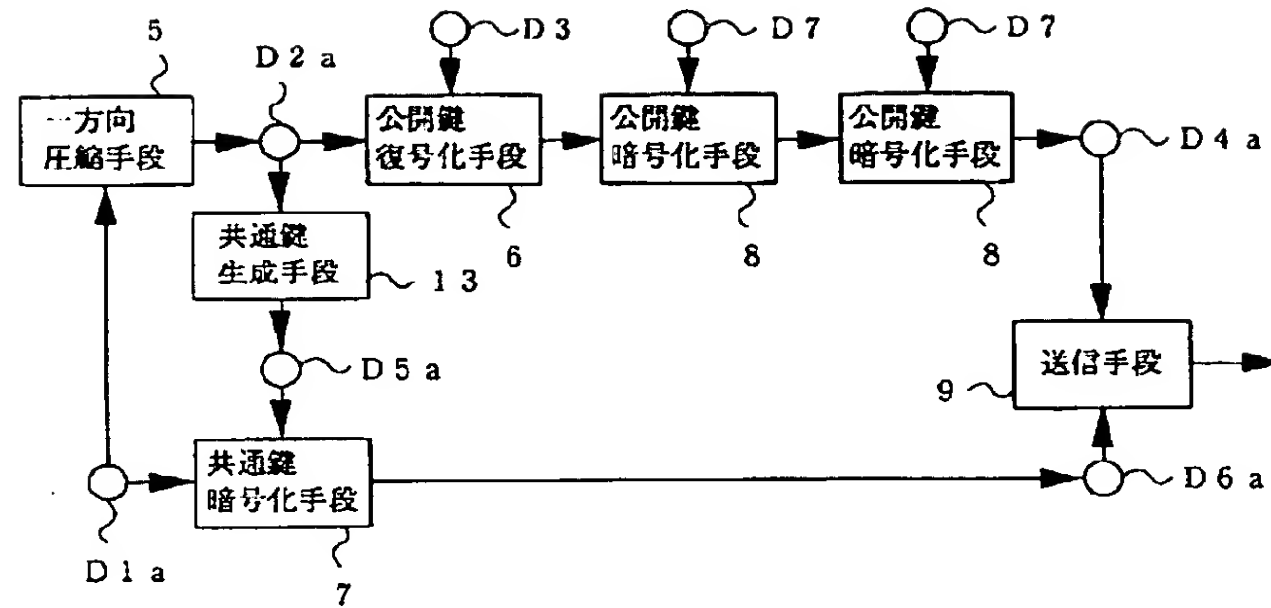
D7 --- 受信者の公開鍵

D9 --- 送信者の公開鍵

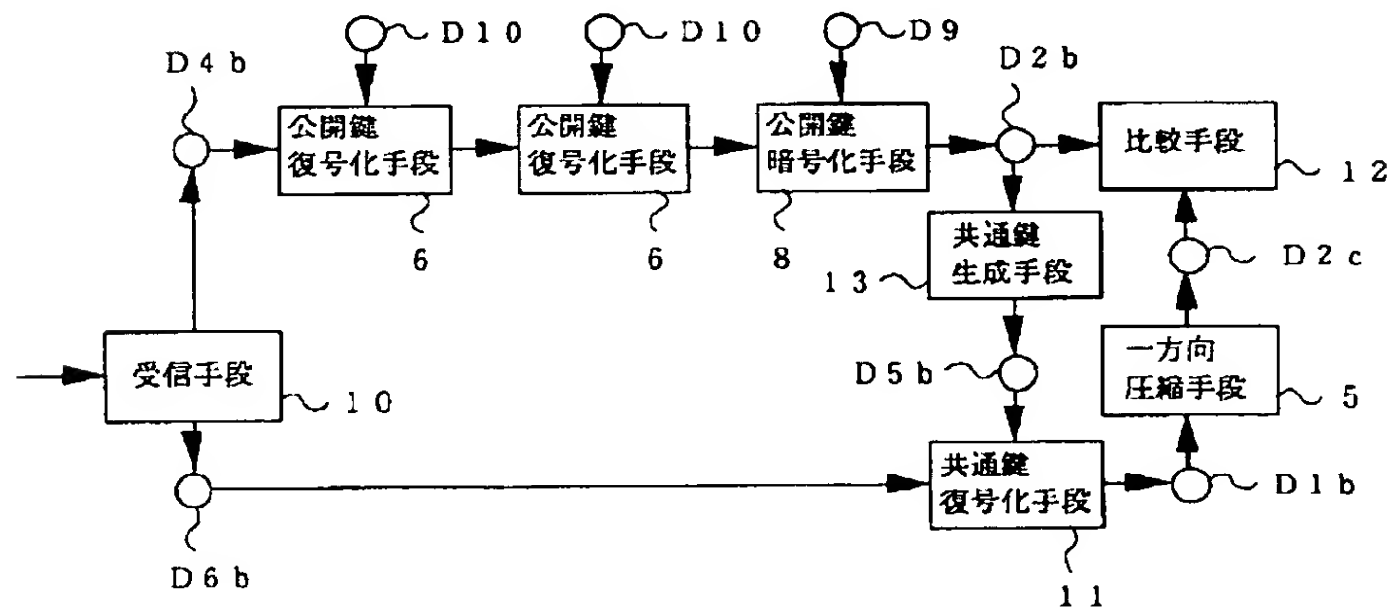
D10 --- 受信者の秘密鍵

【図4】

(a)



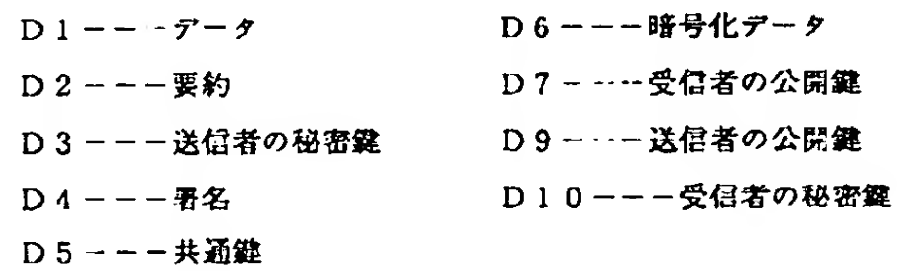
(b)



D1 --- データ
D2 --- 要約
D3 --- 送信者の秘密鍵
D4 --- 署名
D5 --- 共通鍵

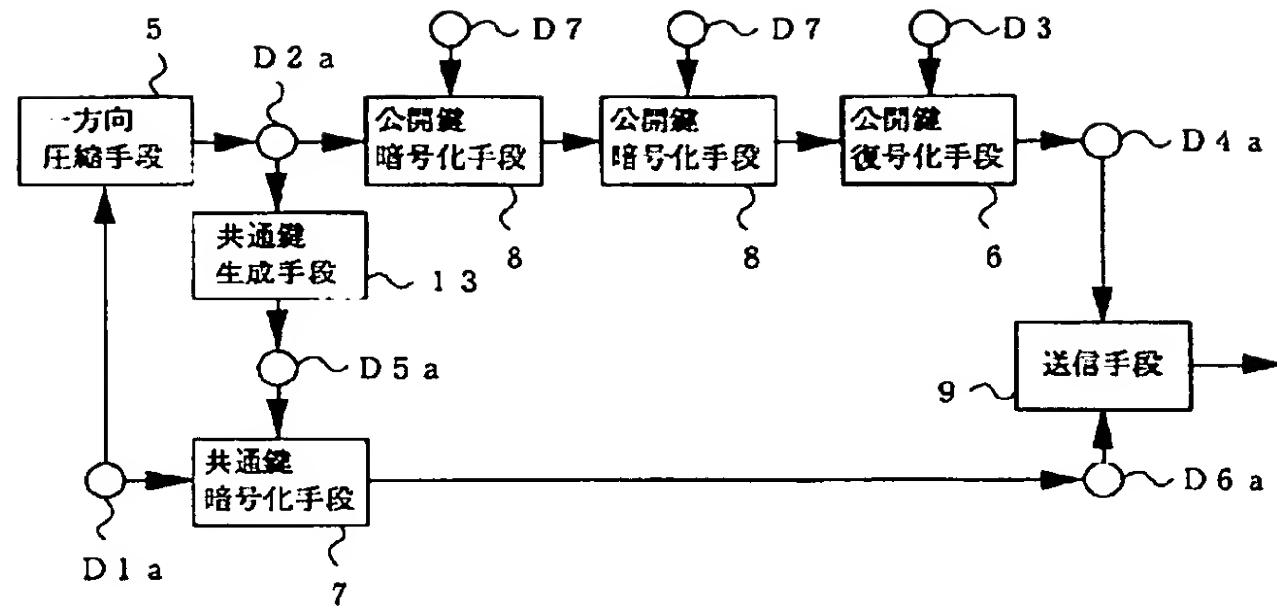
D6 --- 暗号化データ
D7 --- 受信者の公開鍵
D9 --- 送信者の公開鍵
D10 --- 受信者の秘密鍵

(a)

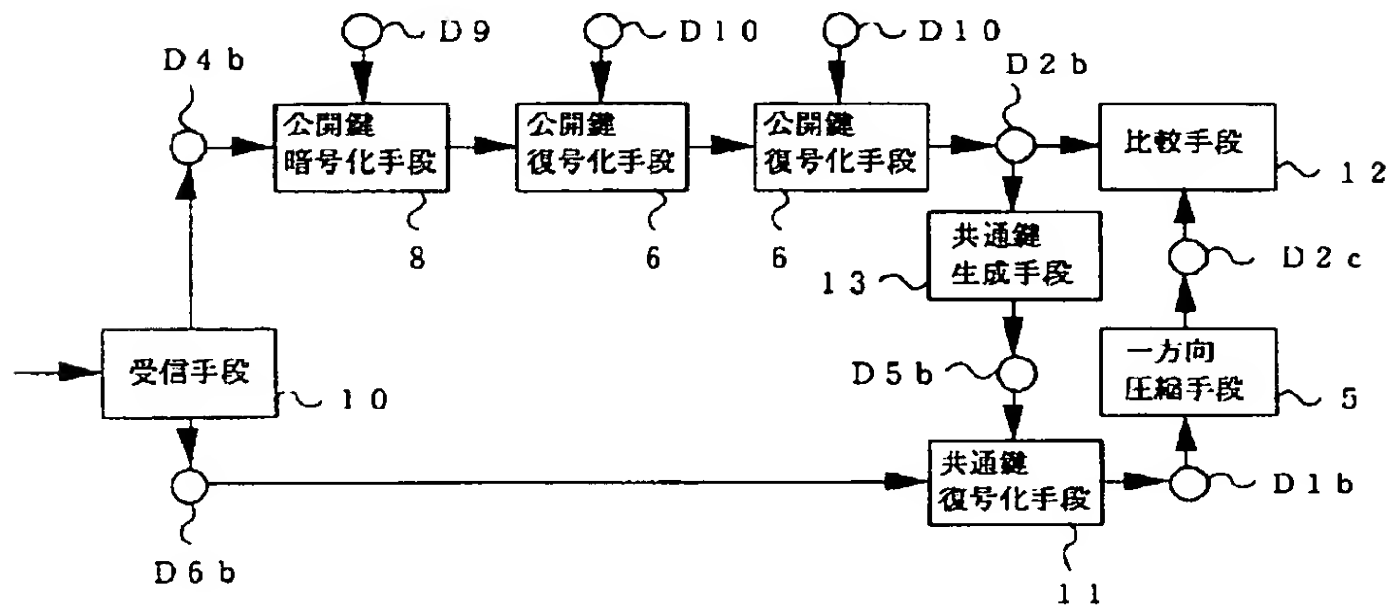


【図6】

(a)



(b)



D1 --- データ

D6 --- 暗号化データ

D2 --- 要約

D7 --- 受信者の公開鍵

D3 --- 送信者の秘密鍵

D9 --- 送信者の公開鍵

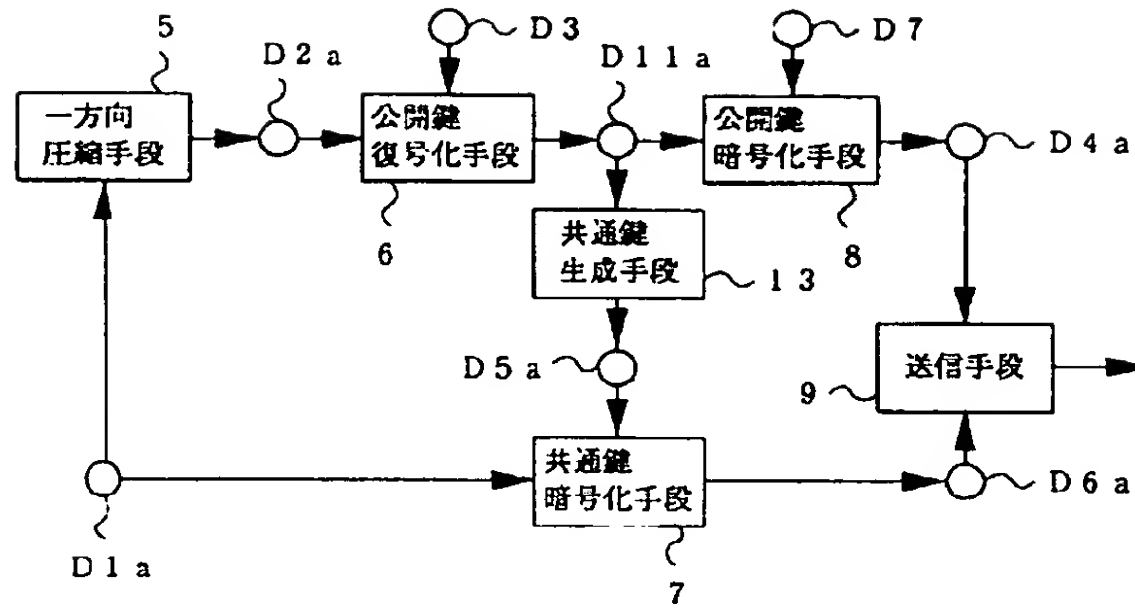
D4 --- 署名

D10 --- 受信者の秘密鍵

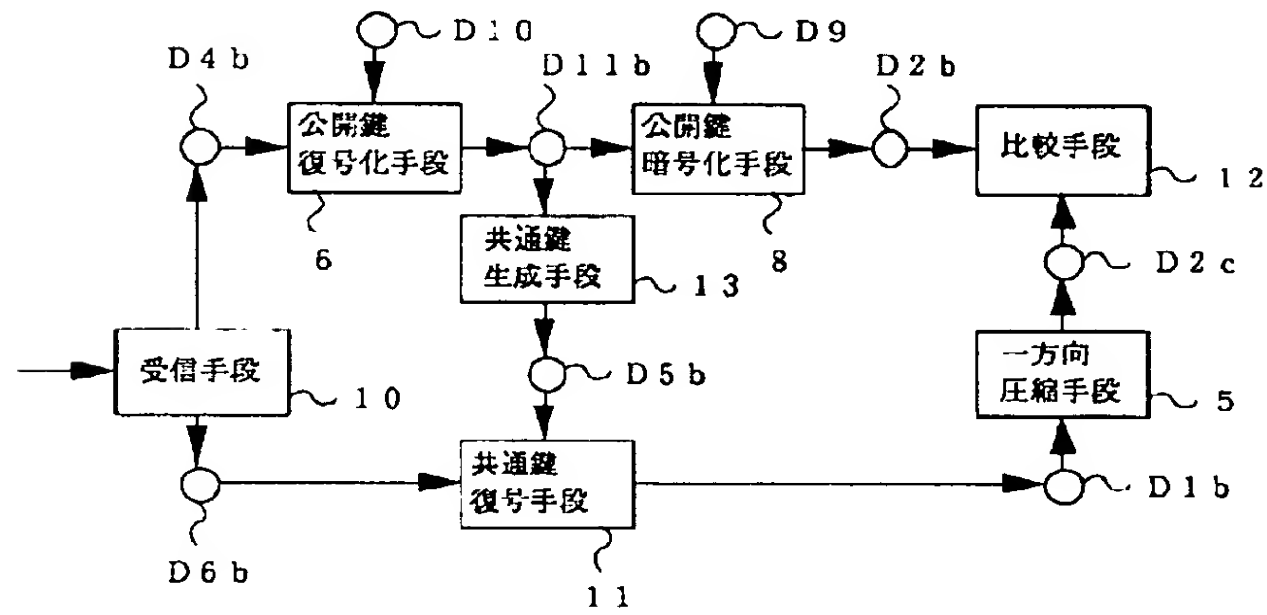
D5 --- 共通鍵

【図7】

(a)



(b)



D1 --- データ

D2 --- 要約

D3 --- 送信者の秘密鍵

D4 --- 署名

D5 --- 共通鍵

D6 --- 暗号化データ

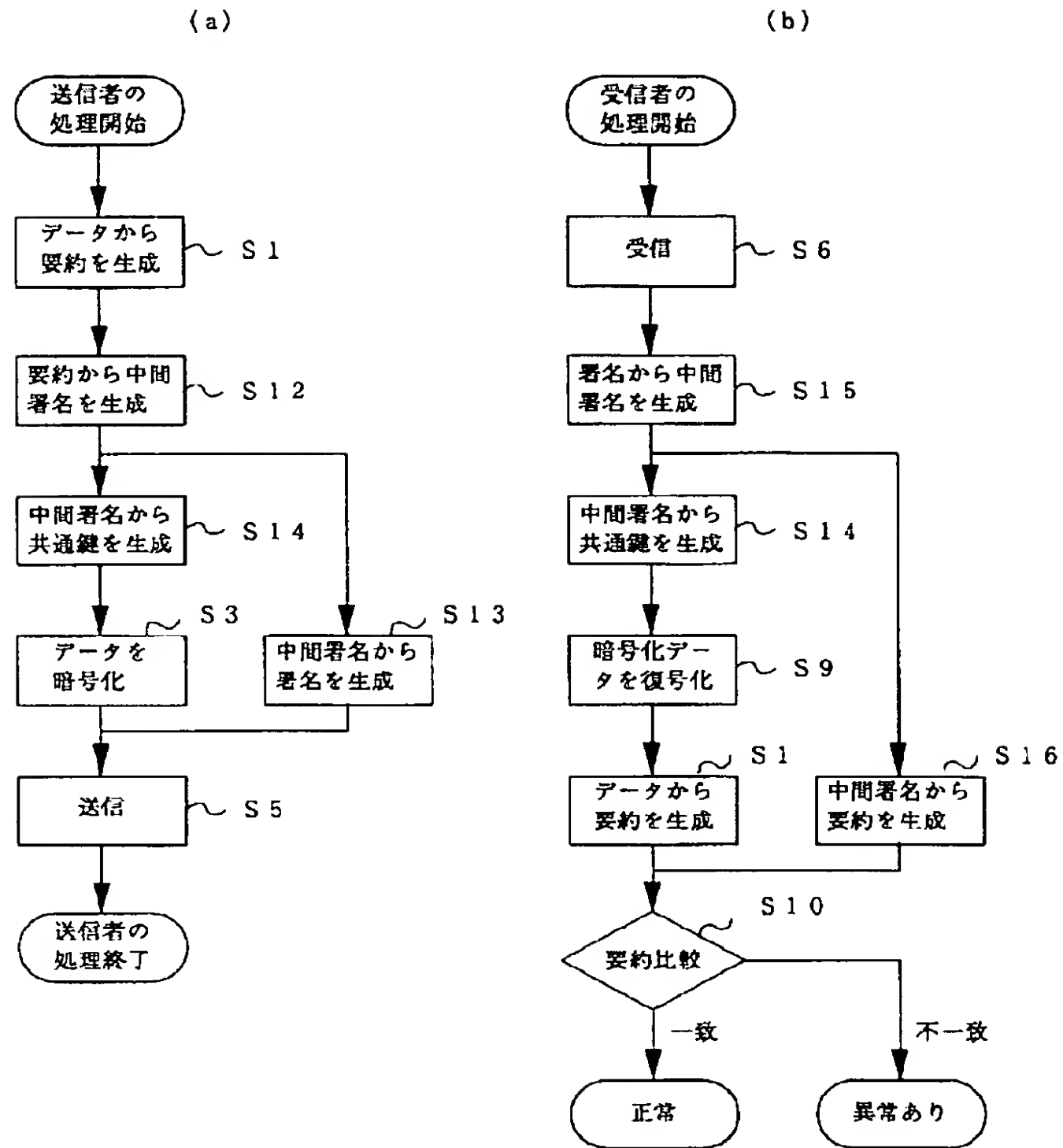
D7 --- 受信者の公開鍵

D9 --- 送信者の公開鍵

D10 --- 受信者の秘密鍵

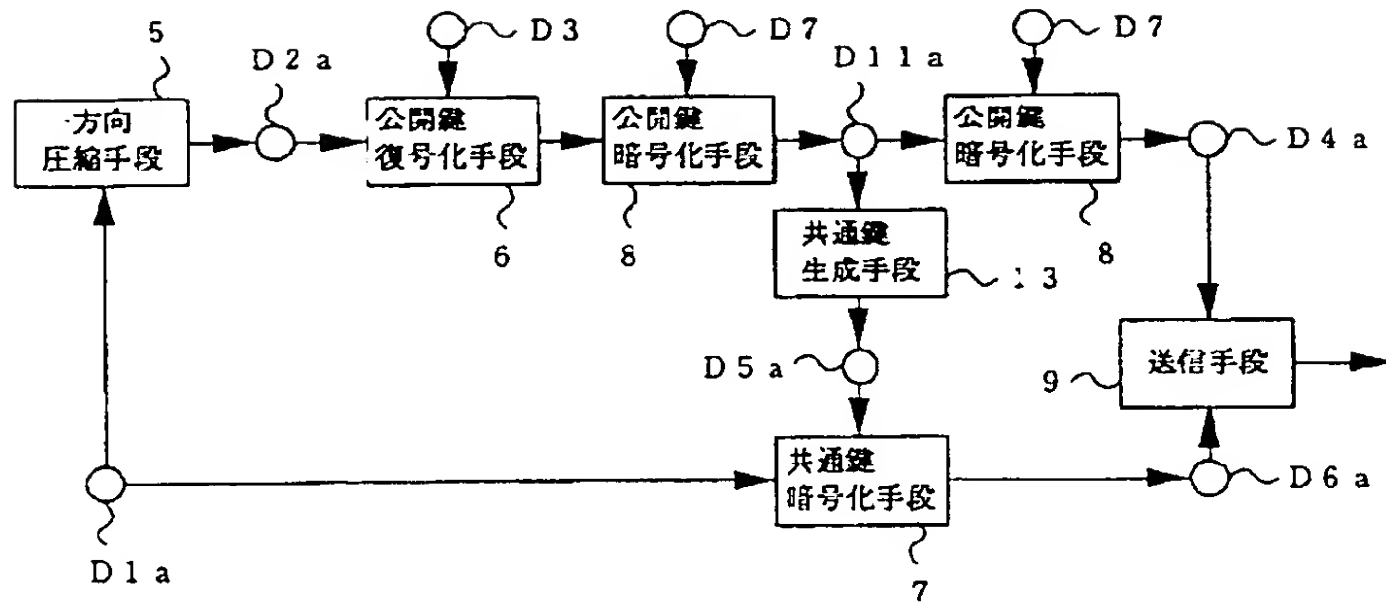
D11 --- 中間署名

【図8】

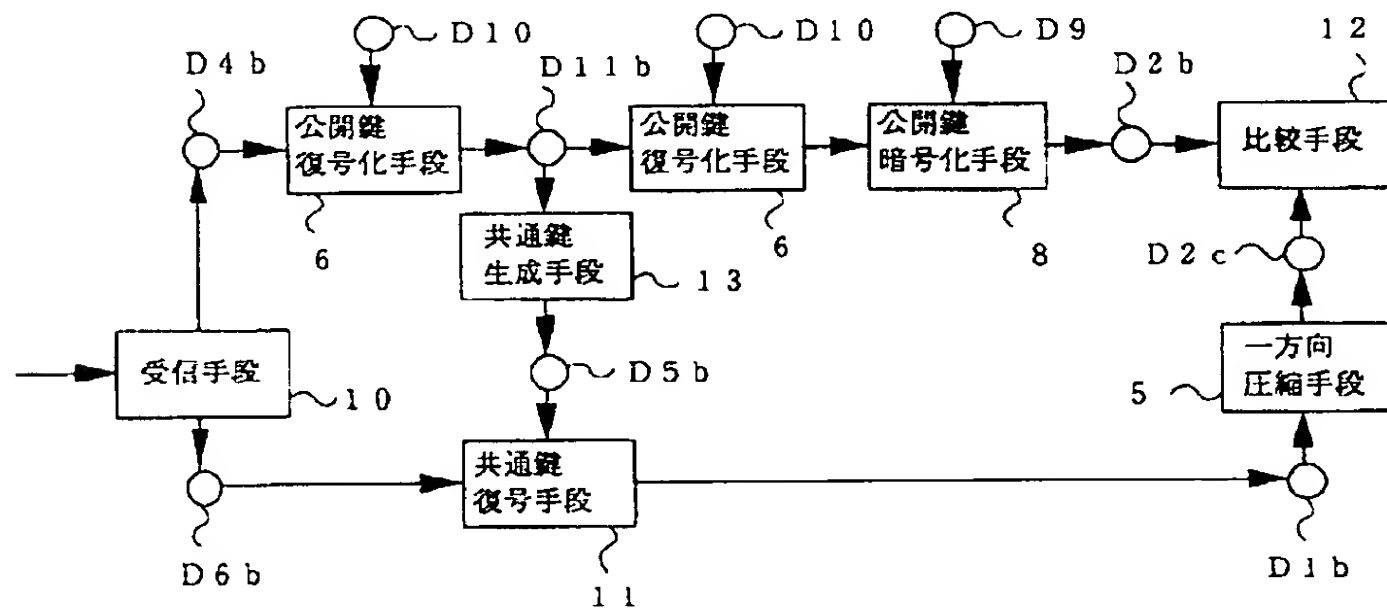


【図9】

(a)



(b)



D1 --- データ

D2 --- 要約

D3 --- 送信者の秘密鍵

D4 --- 署名

D5 --- 共通鍵

D6 --- 暗号化データ

D7 --- 受信者の公開鍵

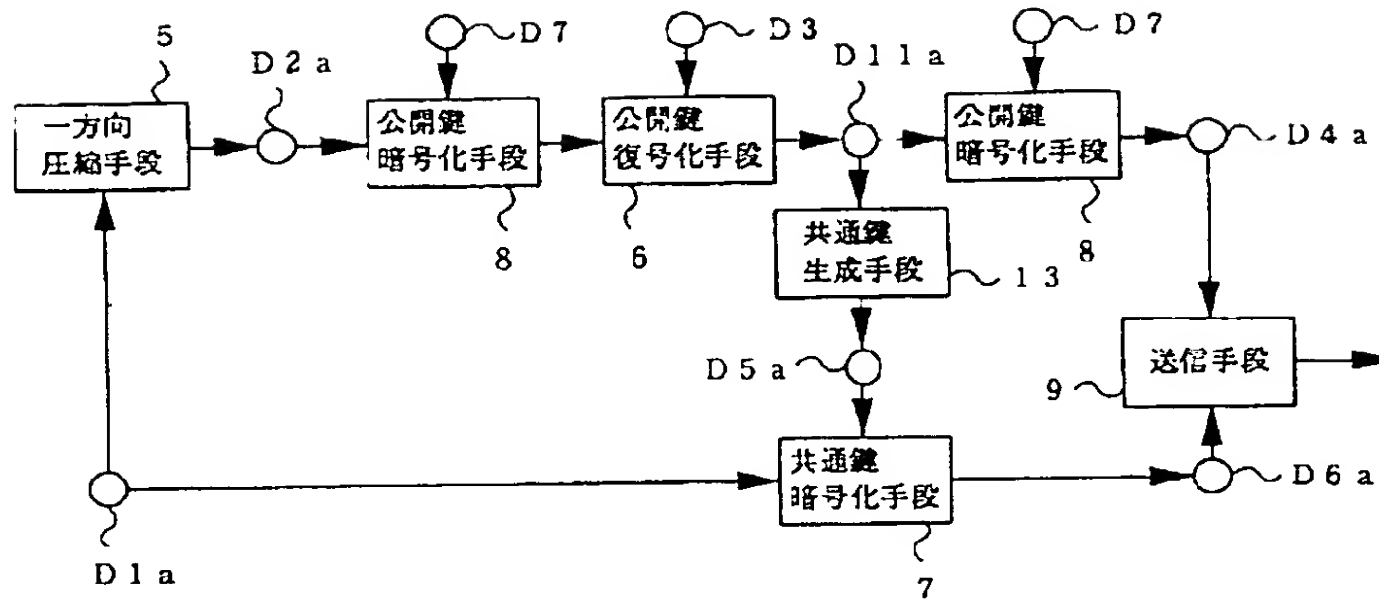
D9 --- 送信者の公開鍵

D10 --- 受信者の秘密鍵

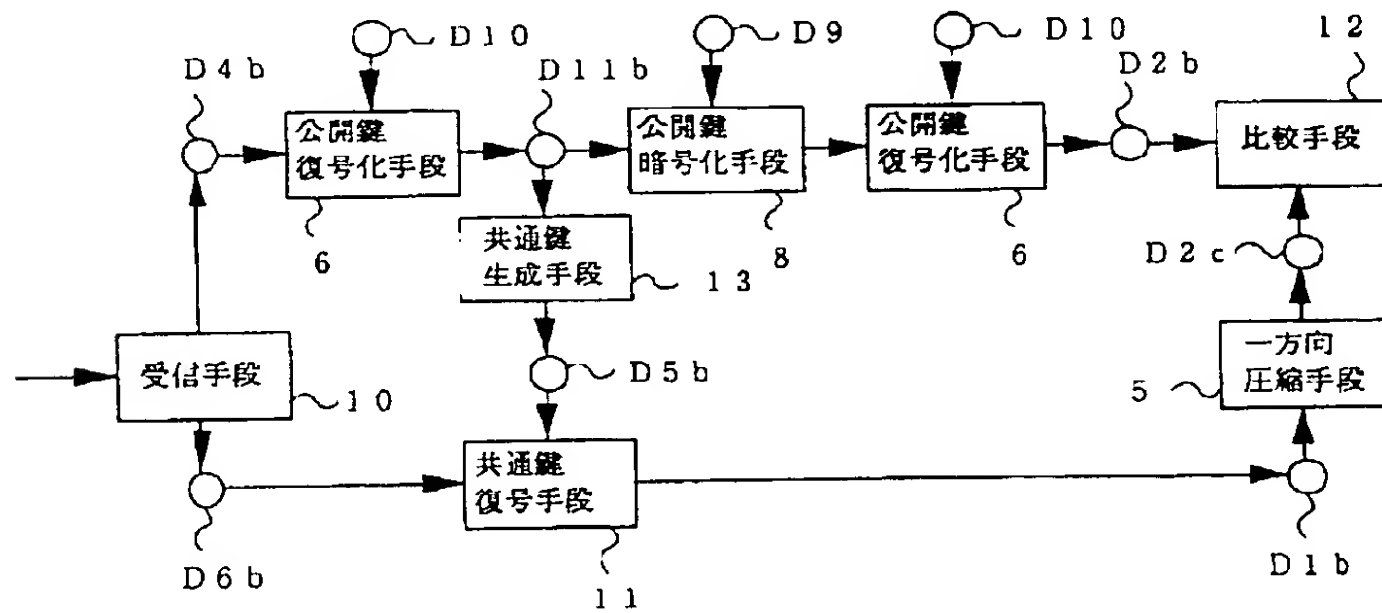
D11 --- 中間署名

【図10】

(a)



(b)

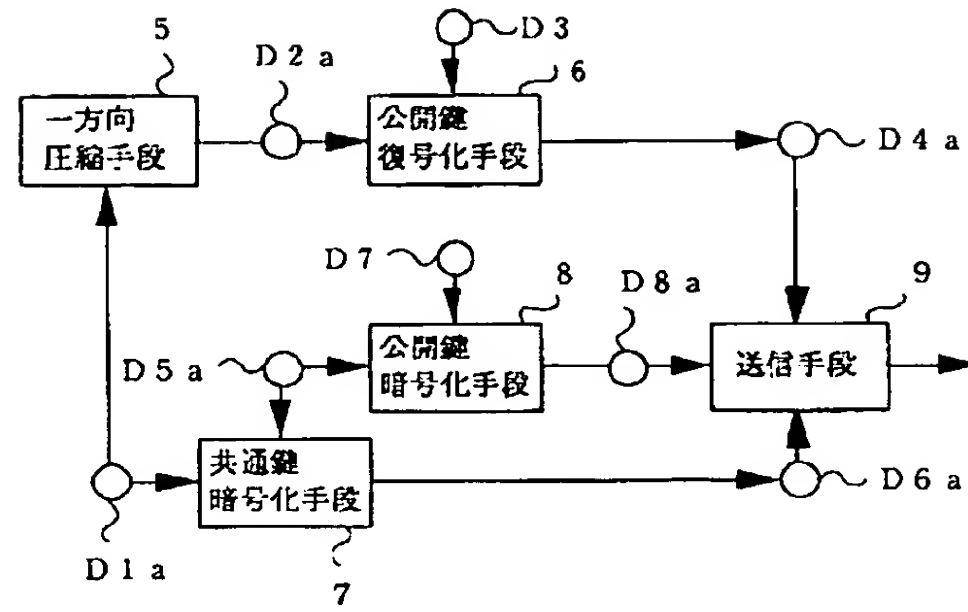


D1 --- データ
 D2 --- 要約
 D3 --- 送信者の秘密鍵
 D4 --- 署名
 D5 --- 共通鍵

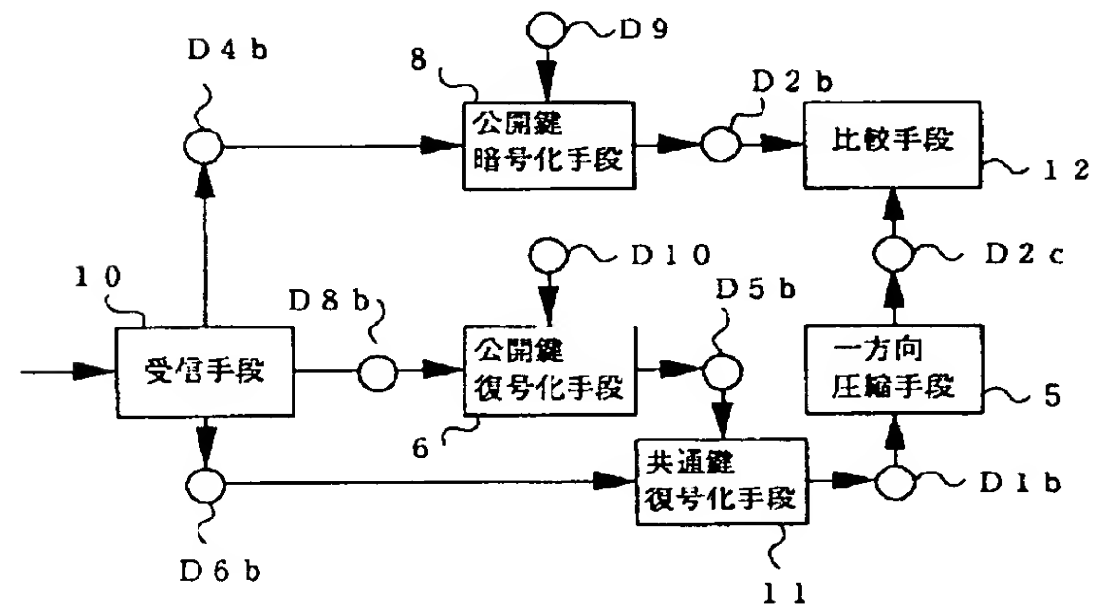
D6 --- 暗号化データ
 D7 --- 受信者の公開鍵
 D9 --- 送信者の公開鍵
 D10 --- 受信者の秘密鍵
 D11 --- 中間署名

【図12】

(a)



(b)



D1 --- データ

D2 --- 要約

D3 --- 送信者の秘密鍵

D4 --- 署名

D5 --- 共通鍵

D6 --- 暗号化データ

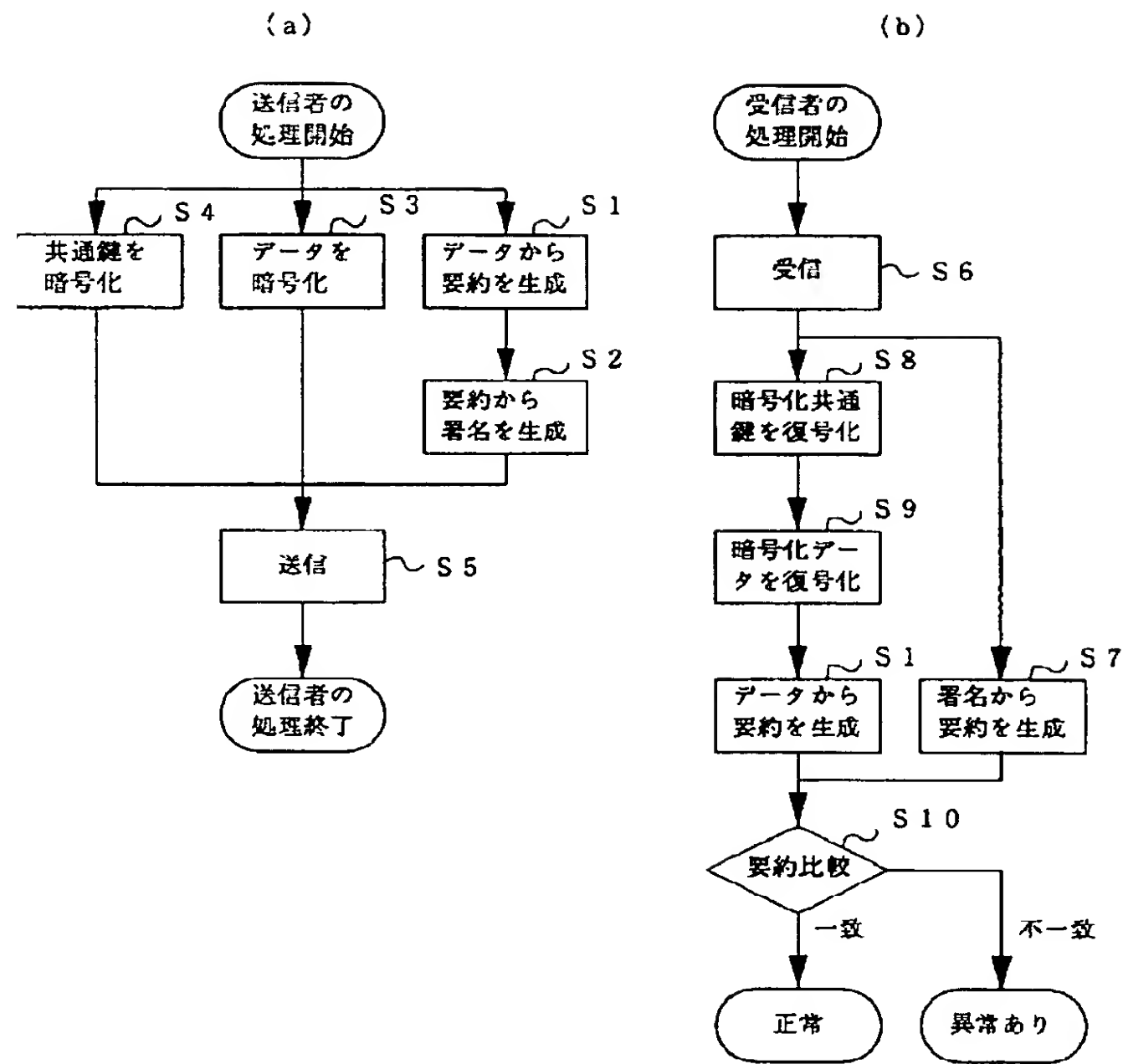
D7 --- 受信者の公開鍵

D8 --- 暗号化共通鍵

D9 --- 送信者の公開鍵

D10 --- 受信者の秘密鍵

【図13】



フロントページの続き

(51)Int.Cl.⁶
H04L 9/08
9/32

識別記号 庁内整理番号

F I
H04L 9/00

技術表示箇所

601C
601E
675B

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.